

A Difference Ring Theory for Symbolic Summation

Carsten Schneider

*Research Institute for Symbolic Computation (RISC)
Johannes Kepler University
Altenbergerstraße 69, 4040 Linz, Austria*

Abstract

A summation framework is developed that enhances Karr's difference field approach. It covers not only indefinite nested sums and products in terms of transcendental extensions, but it can treat, e.g., nested products defined over roots of unity. The theory of the so-called $R\Pi\Sigma^*$ -extensions is supplemented by algorithms that support the construction of such difference rings automatically and that assist in the task to tackle symbolic summation problems. Algorithms are presented that solve parameterized telescoping equations, and more generally parameterized first-order difference equations, in the given difference ring. As a consequence, one obtains algorithms for the summation paradigms of telescoping and Zeilberger's creative telescoping. With this difference ring theory one gets a rigorous summation machinery that has been applied to numerous challenging problems coming, e.g., from combinatorics and particle physics.

Key words: difference ring extensions, roots of unity, indefinite nested sums and products, parameterized telescoping (telescoping, creative telescoping), semi-constants, semi-invariants

1. Introduction

In his pioneering work [24,25] M. Karr introduced a very general class of difference fields, the so-called $\Pi\Sigma$ -fields, in which expressions in terms of indefinite nested sums and products can be represented. In particular, he developed an algorithm that decides constructively if for a given expression $f(k)$ represented in a $\Pi\Sigma$ -field \mathbb{F} there is an expression $g(k)$ represented in the field \mathbb{F} such that the telescoping equation (anti-difference)

$$f(k) = g(k+1) - g(k) \tag{1}$$

* Supported by the Austrian Science Fund (FWF) grant SFB F50 (F5009-N15) and the European Commission through contract PITN-GA-2010-264564 (LHCPhenoNet).

Email address: Carsten.Schneider@risc.jku.at (Carsten Schneider).

holds. If such a solution exists, one obtains for an appropriately chosen $a \in \mathbb{N}$ the identity

$$\sum_{k=a}^b f(k) = g(b+1) - g(a). \quad (2)$$

His algorithms can be viewed as the discrete version of Risch's integration algorithm; see [40,13]. In the last years the $\Pi\Sigma$ -field theory has been pushed forward. It is now possible to obtain sum representations, i.e., right hand sides in (2) with certain optimality criteria such as minimal nesting depth [53,56], minimal number of generators in the summands [45] or minimal degrees in the denominators [51]. For the simplification of products see [48,8]. We emphasize that exactly such refined representations give rise to more efficient telescoping algorithms worked out in [55,59].

A striking application is that Karr's algorithm and all the enhanced versions can be used to solve the parameterized telescoping problem [41,54]: for given indefinite nested product-sum expressions $f_1(k), \dots, f_n(k)$ represented in \mathbb{F} , find constants c_1, \dots, c_n , free of k and not all zero, and find $g(k)$ represented in \mathbb{F} such that

$$g(k+1) - g(k) = c_1 f_1(k) + \dots + c_n f_n(k) \quad (3)$$

holds. In particular, this problem covers Zeilberger's creative telescoping paradigm [62] for a bivariate function $F(m, k)$ by setting $f_i(k) = F(m+i-1, k)$ with $i \in \{1, \dots, n\}$ and representing these $f_i(k)$ in \mathbb{F} . Namely, if one finds such a solution, one ends up at the recurrence

$$g(m, b+1) - g(m, a) = c_1 \sum_{k=a}^b f(m, k) + \dots + c_n \sum_{k=a}^b f(m+n-1, k).$$

In a nutshell, one cannot only treat indefinite summation but also definite summation problems. In this regard, also recurrence solvers have been developed where the coefficients of the recurrence and the inhomogeneous part can be elements from a $\Pi\Sigma$ -field [14,49,6]. All these algorithms generalize and enhance substantially the (q) -hypergeometric and holonomic toolbox [5,18,61,62,36,34,37,35,9,15,26,30] in order to rewrite definite sums to indefinite nested sums. For details on these aspects we refer to [58].

Besides all these sophisticated developments, e.g., within the summation package **Sigma** [52], there is one critical gap which concerns all the developed tools in the setting of difference fields: Algebraic products, like

$$(-1)^k = \prod_{i=1}^k (-1), \quad (-1)^{\binom{k+1}{2}} = \prod_{i=1}^k \prod_{j=1}^i (-1), \quad (-1)^{\binom{k+2}{3}} = \prod_{i=1}^k \prod_{j=1}^i \prod_{k=1}^j (-1), \dots \quad (4)$$

cannot be expressed in $\Pi\Sigma$ -fields, which are built by a tower of transcendental field extensions. Even worse, the objects given in (4) introduce zero-divisors, like

$$(1 - (-1)^k)(1 + (-1)^k) = 0 \quad (5)$$

which cannot be treated in a field or in an integral domain. In applications these objects occur rather frequently as standalone objects or in nested sums [3,4]. It is thus a fundamental challenge to include such objects in an enhanced summation theory.

With the elegant theory of [60,19] one can handle such objects by several copies of the underlying difference field, i.e., by implementing the concept of interlacing in an algebraic way. First steps to combine these techniques with $\Pi\Sigma$ -fields have been made in [17].

Within the package **Sigma** a different approach [42] has been implemented. Summation objects like $(-1)^k$ and sums over such objects are introduced by a tower of generators subject to the relations such as (5). In this way one obtains a direct translation between the summation objects and the generators of the corresponding difference rings. This enhancement has been applied non-trivially, e.g., to combinatorial problems [44,39], number theory [50,33] or to problems from particle physics [12]; for the most recent evaluations of Feynman integrals [11,2,1] up to 300 generators were used to model the summation objects in difference rings. But so far, this successful and very efficient machinery of **Sigma** was built, at least partially, on heuristic considerations.

In this article we shall develop the underlying difference ring theory and supplement it with the missing algorithmic building blocks in order to obtain a rigorous summation machinery. More precisely, we will enhance the difference field theory of [24,25] to a difference ring theory by introducing besides Π -extensions (for transcendental product extensions) and Σ^* -extensions (for transcendental sum extensions) also R -extensions which enables one to represent objects such as (4). An important ingredient of this theory is the exploration of the so-called semi-constants (resp. semi-invariants) and the formulation of the symbolic summation problems within these notions. In particular, we obtain algorithms that can solve certain classes of parameterized first-order linear difference equations. As special instances we obtain algorithms for the parameterized telescoping problem, in particular for the summation paradigms of telescoping and creative telescoping. In addition, we provide an algorithmic toolbox that supports the construction of the so-called simple $R\Pi\Sigma^*$ -extensions automatically. As a special case we demonstrate, how d'Alembertian solutions [7] of a recurrence, a subclass of Liouvillian solutions [20,38], can be represented in such $R\Pi\Sigma^*$ -extensions. In particular, we will illustrate the underlying problems and their solutions by discovering the following identities

$$\sum_{k=1}^b (-1)^{\binom{k+1}{2}} k^2 \sum_{j=1}^k \frac{(-1)^j}{j} = \frac{1}{2} \sum_{j=1}^b \frac{(-1)^{\binom{j+1}{2}}}{j} - \frac{1}{4} (-1)^{\binom{b+1}{2}} (-1 + (-1)^b + 2b) + (-1)^{\binom{b+1}{2}} \frac{1}{2} (b(b+2) + (-1)^b (b^2 - 1)) \sum_{j=1}^b \frac{(-1)^j}{j}, \quad (6)$$

$$\prod_{k=1}^b \frac{-\iota^k}{1+k} = \left(-\frac{\iota}{2} - \frac{1}{2} \right) \frac{-(-1)^b + \iota}{b(b+1)} \left(\prod_{j=1}^{b-1} \frac{\iota^j}{j} \right); \quad (7)$$

here the imaginary unit is denoted by ι , i.e., $\iota^2 = -1$.

The outline is as follows. In Section 2 we will introduce the basic notations of difference rings (resp. fields) and define $R\Pi\Sigma^*$ -ring extensions. Furthermore, we will work out the underlying problems in the setting of difference rings and motivate the different challenges that will be treated in this article. In addition, we give an overview of the main results and show how they can be applied for symbolic summation. In the remaining sections these results will be worked out in details. In Section 3 we present the crucial properties of single nested $R\Pi\Sigma^*$ -extensions. Special emphasis will be put on the properties of the underlying ring. In Section 4 we will consider a tower of such extensions and explore the set of semi-constants. In Section 5 we present algorithms that calculate the order, period and factorial order of the generators of R -extensions. Finally, in Section 6 and Section 7 we elaborate algorithms that are needed to construct $R\Pi\Sigma^*$ -extensions and that solve as a special case the (parameterized) telescoping problem. A conclusion is given in Section 8.

2. Basic definitions, the outline of the problems, and the main results

In this article all rings are commutative with 1 and all rings (resp. fields) have characteristic 0; in particular, they contain the rational numbers \mathbb{Q} as a subring (resp. subfield). A ring (resp. field) is called computable if there are algorithms available that can perform the standard operations (including zero recognition and deciding constructively if an element is invertible). The multiplicative group of units (invertible elements) of a ring \mathbb{A} is denoted by \mathbb{A}^* . The ideal generated by $S \subseteq \mathbb{A}$ is denoted by $\langle S \rangle$. If \mathbb{A} is a subring (resp. subfield/multiplicative subgroup) of $\tilde{\mathbb{A}}$ we also write $\mathbb{A} \leq \tilde{\mathbb{A}}$. The non-negative integers are denoted by $\mathbb{N} = \{0, 1, 2, \dots\}$.

In this section we will present a general framework in which our symbolic summation problems can be formulated and tackled in the setting of difference rings. Here an indefinite nested product-sum expression $f(k)$ (like in (1) or (3)) is described in a ring (resp. field) \mathbb{A} and the shift behaviour of such an expression is reflected by a ring automorphism (resp. field automorphism) $\sigma: \mathbb{A} \rightarrow \mathbb{A}$, i.e., $\sigma^i(f)$ with $i \in \mathbb{Z}$ represents the expression $f(k+i)$. In the following we call such a ring \mathbb{A} (resp. field) equipped with a ring automorphism (resp. field automorphism) σ a difference ring (resp. difference field) [16,31] and denote it by (\mathbb{A}, σ) . We remark that any difference field is also a difference ring. Conversely, any difference ring (\mathbb{A}, σ) with \mathbb{A} being a field is automatically a difference field. A difference ring (resp. field) (\mathbb{A}, σ) is called computable if both, \mathbb{A} and the function σ are computable; note that in such rings one can decide if an element is a constant, i.e., if $\sigma(c) = c$. The set of constants is also denoted by $\text{const}(\mathbb{A}, \sigma) = \{c \in \mathbb{A} \mid \sigma(c) = c\}$, and if it is clear from the context, we also write $\text{const}\mathbb{A} = \text{const}(\mathbb{A}, \sigma)$. It is easy to check that $\text{const}\mathbb{A}$ is a subring (resp. a subfield) of \mathbb{A} which contains as subring (resp. subfield) the rational numbers \mathbb{Q} . Throughout this article we will take care that $\text{const}\mathbb{A}$ is always a field (and not just a ring), called the constant field and denoted by \mathbb{K} .

In the first subsection we introduce the class of difference rings in which we will model indefinite nested sums and products. They will be introduced by a tower of ring extensions, the so-called $R\Pi\Sigma^*$ -ring extensions.

In Subsection 2.2 we will focus on two tasks:

- (1) Introduce techniques that enable one to test if the given tower of extensions is an $R\Pi\Sigma^*$ -extension; even more, derive tactics that enable one to represent sums and products automatically in $R\Pi\Sigma^*$ -extensions.
- (2) Work out the underlying subproblems in order to solve two central problems of symbolic summation: telescoping (compare (1)) and parameterized telescoping (compare (3)). In their simplest form they can be specified as follows.

Problem T for (\mathbb{A}, σ) . *Given a difference ring (\mathbb{A}, σ) and given $f \in \mathbb{A}$. Find, if possible, a $g \in \mathbb{A}$ such that the telescoping (T) equation holds:*

$$\sigma(g) - g = f. \quad (8)$$

Problem PT for (\mathbb{A}, σ) . *Given a difference ring (\mathbb{A}, σ) with constant field \mathbb{K} and given $f_1, \dots, f_n \in \mathbb{A}$. Find, if possible, $c_1, \dots, c_n \in \mathbb{K}$ (not all c_i being zero) and a $g \in \mathbb{A}$ such that the parameterized telescoping (PT) holds:*

$$\sigma(g) - g = c_1 f_1 + \dots + c_n f_n. \quad (9)$$

In Subsection 2.3 we will present the main results of theoretical and algorithmic nature to handle these problems, and in Subsection 2.4 we demonstrate how the new summation theory can be used to represent d'Alembertian solutions in $R\Pi\Sigma^*$ -extensions.

2.1. The definition of $R\Pi\Sigma^*$ -extensions

A difference ring $(\tilde{\mathbb{A}}, \tilde{\sigma})$ is a difference ring extension of a difference ring (\mathbb{A}, σ) if $\mathbb{A} \leq \tilde{\mathbb{A}}$ and $\tilde{\sigma}|_{\mathbb{A}} = \sigma$, i.e., \mathbb{A} is a subring of $\tilde{\mathbb{A}}$ and $\tilde{\sigma}(a) = \sigma(a)$ for all $a \in \mathbb{A}$. The definition of difference field extensions is the same by replacing the word ring with field. In short (for the ring and field version) we also write $(\mathbb{A}, \sigma) \leq (\tilde{\mathbb{A}}, \tilde{\sigma})$. If it is clear from the context, we do not distinguish anymore between σ and $\tilde{\sigma}$.

For the construction of $R\Pi\Sigma^*$ -extensions, we start with the following basic properties.

Lemma 2.1. Let \mathbb{A} be a ring with $\alpha \in \mathbb{A}^*$ and $\beta \in \mathbb{A}$ equipped with a ring automorphism $\sigma: \mathbb{A} \rightarrow \mathbb{A}$. Let $\mathbb{A}[t]$ be a polynomial ring and $\mathbb{A}[t, \frac{1}{t}]$ be a ring of Laurent polynomials.

- (1) There is a unique automorphism $\sigma': \mathbb{A}[t] \rightarrow \mathbb{A}[t]$ with $\sigma'|_{\mathbb{A}} = \sigma$ and $\sigma'(t) = \alpha t + \beta$.
- (2) There is a unique automorphism $\sigma'': \mathbb{A}[t, \frac{1}{t}] \rightarrow \mathbb{A}[t, \frac{1}{t}]$ with $\sigma''|_{\mathbb{A}} = \sigma$ and $\sigma''(t) = \alpha t$ (where $\sigma''(\frac{1}{t}) = \alpha^{-1} \frac{1}{t}$). In particular, if $\beta = 0$, $\sigma''|_{\mathbb{A}[t]} = \sigma'$.
- (3) If \mathbb{A} is field and $\mathbb{A}(t)$ is a rational function field, there is a unique field automorphism $\sigma''': \mathbb{A}(t) \rightarrow \mathbb{A}(t)$ with $\sigma'''|_{\mathbb{A}} = \sigma$ and $\sigma'''(t) = \alpha t + \beta$. In particular, $\sigma'''|_{\mathbb{A}[t]} = \sigma'$; moreover, $\sigma'''|_{\mathbb{A}[t, 1/t]} = \sigma''$ if $\beta = 0$.

In summary, let (\mathbb{A}, σ) be a difference ring and t be transcendental over \mathbb{A} . Then we obtain the uniquely determined difference ring extension $(\mathbb{A}[t], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t + \beta$ where $\alpha \in \mathbb{A}^*$ and $\beta \in \mathbb{A}$. In particular, we get the uniquely determined difference ring extension $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$. Thus for $\beta = 0$, we have the chain of extensions $(\mathbb{A}, \sigma) \leq (\mathbb{A}[t], \sigma) \leq (\mathbb{A}[t, \frac{1}{t}], \sigma)$. Moreover, if \mathbb{A} is a field, we obtain the uniquely determined difference field extension $(\mathbb{A}(t), \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t + \beta$. Following the notions of [14] each of the extensions, i.e., $(\mathbb{A}, \sigma) \leq (\mathbb{A}[t], \sigma)$, $(\mathbb{A}, \sigma) \leq (\mathbb{A}[t, \frac{1}{t}], \sigma)$ or $(\mathbb{A}, \sigma) \leq (\mathbb{A}(t), \sigma)$ are called unimonomial extensions (of polynomial, Laurent polynomial or of rational function type, respectively).

Example 2.2. (0) Take the difference field (\mathbb{Q}, σ) with $\sigma(c) = c$ for all $c \in \mathbb{Q}$.

- (1) Take the unimonomial field extension $(\mathbb{Q}(k), \sigma)$ of (\mathbb{Q}, σ) with $\sigma(k) = k + 1$: $\mathbb{Q}(k)$ is a rational function field and σ is extended from \mathbb{Q} to $\mathbb{Q}(k)$ with $\sigma(k) = k + 1$.
- (2) Take the unimonomial ring extension $(\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ of $(\mathbb{Q}(k), \sigma)$ with $\sigma(t) = (k + 1)t$: $\mathbb{Q}(k)[t, \frac{1}{t}]$ is a ring of Laurent polynomials with coefficients from $\mathbb{Q}(k)$ and the automorphism is extended from $\mathbb{Q}(k)$ to $\mathbb{Q}(k)[t, \frac{1}{t}]$ with $\sigma(t) = (k + 1)t$.

Finally, we consider those extensions where the constants remain unchanged.

Definition 2.3. Let (\mathbb{A}, σ) be a difference ring.

- A unimonomial ring extension $(\mathbb{A}[t], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) - t \in \mathbb{A}$ and $\text{const} \mathbb{A}[t] = \text{const} \mathbb{A}$ is called Σ^* -ring extension (in short Σ^* -extension).
- If \mathbb{A} is a field, a unimonomial field extension $(\mathbb{A}(t), \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) - t \in \mathbb{A}$ and $\text{const} \mathbb{A}(t) = \text{const} \mathbb{A}$ is called Σ^* -field¹ extension.

¹ We restrict Karr's Σ -field extensions to Σ^* -field extensions being slightly less general but covering all sums treated explicitly in Karr's work [24].

- A unimonomial ring extension $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ of (\mathbb{A}, σ) with $\frac{\sigma(t)}{t} \in \mathbb{A}^*$ and $\text{const} \mathbb{A}[t, \frac{1}{t}] = \text{const} \mathbb{A}$ is called Π -ring extension (in short Π -extension).
- If \mathbb{A} is a field, a unimonomial field extension $(\mathbb{A}(t), \sigma)$ of (\mathbb{A}, σ) with $\frac{\sigma(t)}{t} \in \mathbb{A}^* = \mathbb{A}(t) \setminus \{0\}$ and $\text{const} \mathbb{A}(t) = \text{const} \mathbb{A}$ is called Π -field extension.

The generators of a Σ^* -extension (in the ring or field version) and a Π -extension (in the ring or field version) are called Σ^* -monomial and Π -monomial, respectively.

Remark 2.4. Keeping the constants unchanged is a central property to tackle the (parameterized) telescoping problem. E.g., if the constants are extended, there do not exist bounds on the degrees as utilized in Subsection 7.1.1. Additionally, introducing no extra constants is *the* essential property to embed the derived difference rings into the ring of sequences; this fact has been worked out, e.g., in [54] which is related to [19].

Example 2.5 (Cont. Ex. 2.2). For $(\mathbb{Q}, \sigma) \leq (\mathbb{Q}(k), \sigma) \leq (\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ from Example 2.2 we have that $\text{const} \mathbb{Q}(k)[t, \frac{1}{t}] = \text{const} \mathbb{Q}(k) = \text{const} \mathbb{Q} = \mathbb{Q}$, which can be checked easily. Thus $(\mathbb{Q}(k), \sigma)$ is a Σ^* -field extension of (\mathbb{Q}, σ) and $(\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ is a Π -extension of $(\mathbb{Q}(k), \sigma)$. The generator k is a Σ^* -monomial and the generator t is a Π -monomial.

For more complicated extensions it is rather demanding to check if the constants remain unchanged. In this regard, we refer to the field-algorithms given in [24] or to our enhanced ring-algorithms given below which can perform these checks automatically.

For further considerations we introduce the order function $\text{ord}: \mathbb{A} \rightarrow \mathbb{N}$ with

$$\text{ord}(h) = \begin{cases} 0 & \text{if } \nexists n > 0 \text{ s.t. } h^n = 1 \\ \min\{n > 0 \mid h^n = 1\} & \text{otherwise.} \end{cases} \quad (10)$$

The third type of extensions is concerned with algebraic objects like (4). Let $\lambda \in \mathbb{N}$ with $\lambda > 1$, take a root of unity $\alpha \in \mathbb{A}^*$ with $\alpha^\lambda = 1$ and construct the unimonomial extension $(\mathbb{A}[y], \sigma)$ of (\mathbb{A}, σ) with $\sigma(y) = \alpha y$. Now take the ideal $I := \langle y^\lambda - 1 \rangle$ and consider the quotient ring $\mathbb{E} = \mathbb{A}[y]/I$. Since I is closed under σ , i.e., I is a reflexive difference ideal [16, page 71], one can verify that $\sigma: \mathbb{E} \rightarrow \mathbb{E}$ with $\sigma(f + I) = \sigma(f) + I$ forms a ring automorphism. In other words, (\mathbb{E}, σ) is a difference ring. Moreover, there is the natural embedding of \mathbb{A} into \mathbb{E} with $a \rightarrow a + I$. By identifying a with $a + I$, (\mathbb{E}, σ) is a difference ring extension of (\mathbb{A}, σ) .

Lemma 2.6. Let (\mathbb{A}, σ) be a difference ring and $\alpha \in \mathbb{A}^*$ with $\alpha^\lambda = 1$ for some $\lambda > 1$. Then there is (up to a difference ring isomorphism) a unique difference ring extension $(\mathbb{A}[x], \sigma)$ of (\mathbb{A}, σ) with $x \notin \mathbb{A}$ subject to the relations $x^\lambda = 1$ and $\sigma(x) = \alpha x$.

Proof. Consider the difference ring extension (\mathbb{E}, σ) of (\mathbb{A}, σ) constructed above. Define $x := y + I$. Then $\sigma(x) = \alpha x$ and $x^\lambda = y^\lambda + I = 1 + I = 1$. Further, $\mathbb{E} = \{\sum_{i=0}^{\lambda-1} a_i x^i \mid a_i \in \mathbb{A}\}$. Thus we obtain a difference ring extension as claimed in the lemma. Now suppose that there is another difference ring extension $(\mathbb{A}[x'], \sigma')$ of (\mathbb{A}, σ) with $x' \notin \mathbb{A}$ subject to the relations $\sigma'(x') = \alpha x'$ and $x'^\lambda = 1$. Then by the first isomorphism theorem, there is the ring isomorphism $\tau: \mathbb{E} \rightarrow \mathbb{A}[x']$ with $\tau(\sum_{i=0}^{\lambda-1} f_i x^i) = \sum_{i=0}^{\lambda-1} f_i x'_i$. Since $\tau(\sigma(x)) = \tau(\alpha x) = \tau(\alpha) \tau(x) = \alpha x' = \sigma'(x')$, it follows that $\tau(\sigma(f)) = \sigma'(\tau(f))$ for all $f \in \mathbb{A}[x]$. Summarizing, τ is a difference ring isomorphism. \square

The extension $(\mathbb{A}[x], \sigma)$ of (\mathbb{A}, σ) in Lemma 2.6 is called algebraic extension of order λ .

Example 2.7. (0) Take the Σ^* -ext. $(\mathbb{Q}(k), \sigma)$ of (\mathbb{Q}, σ) with $\sigma(k) = k + 1$ from Ex. 2.5.
(1) Take the algebraic extension $(\mathbb{Q}(k)[x], \sigma)$ of $(\mathbb{Q}(k), \sigma)$ with $\sigma(x) = -x$ of order 2: $\mathbb{Q}(k)[x]$ is an algebraic ring extension of $\mathbb{Q}(k)$ subject to the relation $x^2 = 1$ and σ is extended from $\mathbb{Q}(k)$ to $\mathbb{Q}(k)[x]$ with $\sigma(x) = -x$. Note that x represents the expression $X(k) = (-1)^k$ with $X(k+1) = -X(k)$.
(2) Take the algebraic extension $(\mathbb{Q}(k)[x][y], \sigma)$ of $(\mathbb{Q}(k)[x], \sigma)$ with $\sigma(y) = -xy$ of order 2: $\mathbb{Q}(k)[x][y]$ is a ring extension of $\mathbb{Q}(k)[x]$ with $y^2 = 1$ and σ is extended from $\mathbb{Q}(k)[x]$ to $\mathbb{Q}(k)[x][y]$ with $\sigma(y) = -xy$. Note that y represents the expression $Y(k) = (-1)^{\binom{k+1}{2}} = \prod_{j=1}^k (-1)^j$ with $Y(k+1) = -(-1)^k Y(k)$.

As for unimonomial extensions, we restrict now to those algebraic extensions where the constants remain unchanged. For the underlying motivation we refer to Remark 2.4.

Definition 2.8. Let $\lambda \in \mathbb{N} \setminus \{0, 1\}$. An algebraic extension $(\mathbb{A}[x], \sigma)$ of (\mathbb{A}, σ) order λ with $\text{const} \mathbb{A}[x] = \text{const} \mathbb{A}$ is called root of unity extension (in short R -extension) of order λ . The generator x is called R -monomial.

Example 2.9 (Cont. Ex. 2.7). For $(\mathbb{Q}, \sigma) \leq (\mathbb{Q}(k), \sigma) \leq (\mathbb{Q}(k)[x], \sigma) \leq (\mathbb{Q}(k)[x][y], \sigma)$ from Example 2.7 we have that $\text{const} \mathbb{Q}(k)[x][y] = \text{const} \mathbb{Q}(k)[x] = \text{const} \mathbb{Q}(k) = \mathbb{Q}$, which can be checked algorithmically; see Example 2.13 below. Thus $(\mathbb{Q}(k)[x], \sigma)$ is an R -extension of $(\mathbb{Q}(k), \sigma)$ and $(\mathbb{Q}(k)[x][y], \sigma)$ is an R -extension of $(\mathbb{Q}(k)[x], \sigma)$.

To this end, we define a tower of such extensions. First, we introduce the following notion. Let $(\mathbb{A}, \sigma) \leq (\mathbb{E}, \sigma)$ with $t \in \mathbb{E}$. In the following $\mathbb{A}\langle t \rangle$ denotes the polynomial ring $\mathbb{A}[t]$ if $(\mathbb{A}[t], \sigma)$ is a Σ^* -extension of (\mathbb{A}, σ) . $\mathbb{A}\langle t \rangle$ denotes the ring of Laurent polynomials $\mathbb{A}[t, \frac{1}{t}]$ if $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ is a Π -extension of (\mathbb{A}, σ) . Finally, $\mathbb{A}\langle t \rangle$ denotes the ring $\mathbb{A}[t]$ with $t \notin \mathbb{A}$ subject to the relation $t^\lambda = 1$ if $(\mathbb{A}[t], \sigma)$ is an R -extension of (\mathbb{A}, σ) of order λ .

Definition 2.10. A difference ring extension $(\mathbb{A}\langle t \rangle, \sigma)$ of (\mathbb{A}, σ) is called $R\Pi\Sigma^*$ -extension if it is an R -extension, Π -extension or Σ^* -extension. Analogously, it is called $R\Sigma^*$ -extension, $R\Pi$ -extension or $\Pi\Sigma^*$ -extension if it is one of the corresponding extensions. More generally, $(\mathbb{G}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_e \rangle, \sigma)$ is a (nested) $R\Pi\Sigma^*$ -extension (resp. $R\Pi$, $R\Sigma^*$, $\Pi\Sigma^*$ -, R -, Π -, Σ^* -extension) of (\mathbb{G}, σ) if it is a tower of such extensions.

Similarly, if \mathbb{A} is a field, $(\mathbb{A}(t), \sigma)$ is called a $\Pi\Sigma^*$ -field extension if it is either a Π -field extension or a Σ^* -field extension. $(\mathbb{G}(t_1) \dots (t_e), \sigma)$ is called a $\Pi\Sigma^*$ -field extension (resp. Π -field extension, Σ^* -field extension) of (\mathbb{G}, σ) if it is a tower of such extensions. In particular, if $\text{const} \mathbb{G} = \mathbb{G}$, $(\mathbb{G}(t_1)(t_2) \dots (t_e), \sigma)$ is called a $\Pi\Sigma^*$ -field over \mathbb{G} .

In both, the ring and field version, t_i is called $R\Pi\Sigma^*$ -monomial (resp. $R\Pi$ -, $R\Sigma^*$ -, $\Pi\Sigma^*$ -monomial) if it is a generator of a $R\Pi\Sigma^*$ -extension (resp. $R\Pi$ -, $R\Sigma^*$ -, $\Pi\Sigma^*$ -extension).

Example 2.11 (Cont. Ex. 2.9). (1) $(\mathbb{Q}(k), \sigma)$ is a $\Pi\Sigma^*$ -field over \mathbb{Q} .
(2) $(\mathbb{Q}(k)\langle x \rangle \langle y \rangle, \sigma)$ is an R -extension of $(\mathbb{Q}(k), \sigma)$.

The generators with their sequential arrangement, incorporating the recursive definition of the automorphism, are always given explicitly. In particular, any reordering of the generators must respect the recursive nature induced by the automorphism.

2.2. A characterization of $R\Pi\Sigma^*$ -extensions and their algorithmic construction

For the construction of $R\Pi\Sigma^*$ -extensions we rely on the following result; for the proofs of part 1, part 2 and part 3 we refer to Proof 3.9, Proof 3.16 and Proof 3.22, respectively.

Theorem 2.12. Let (\mathbb{A}, σ) be a difference ring. Then the following holds.

- (1) Let $(\mathbb{A}[t], \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) with $\sigma(t) = t + \beta$ where $\beta \in \mathbb{A}$ such that $\text{const}\mathbb{A}$ is a field. Then this is a Σ^* -extension (i.e., $\text{const}\mathbb{A}[t] = \text{const}\mathbb{A}$) iff there does not exist a $g \in \mathbb{A}$ with $\sigma(g) = g + \beta$.
- (2) Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ where $\alpha \in \mathbb{A}^*$. Then this is a Π -extension (i.e., $\text{const}\mathbb{A}[t, \frac{1}{t}] = \text{const}\mathbb{A}$) iff there are no $g \in \mathbb{A} \setminus \{0\}$ and $m \in \mathbb{Z} \setminus \{0\}$ with $\sigma(g) = \alpha^m g$. If it is a Π -extension, $\text{ord}(\alpha) = 0$.
- (3) Let $(\mathbb{A}[t], \sigma)$ be an algebraic ring extension of (\mathbb{A}, σ) of order $\lambda > 1$ with $\sigma(t) = \alpha t$ where $\alpha \in \mathbb{A}^*$. Then this is an R -extension (i.e., $\text{const}\mathbb{A}[t] = \text{const}\mathbb{A}$) iff there are no $g \in \mathbb{A} \setminus \{0\}$ and $m \in \{1, \dots, \lambda - 1\}$ with $\sigma(g) = \alpha^m g$. If it is an R -extension, then α is primitive, i.e., $\text{ord}(\alpha) = \lambda$.

For Karr's celebrated field version [24,25] of this result we refer to Theorems 3.11 and 3.18 below, that can be nicely embedded in the general difference ring framework. We emphasize that Theorem 2.12 facilitates algorithmic tactics to build difference ring extensions and to verify simultaneously if they form $R\Pi\Sigma^*$ -extensions. Here we consider two cases.

2.2.1. Testing and constructing $R\Pi$ -extensions

Let (\mathbb{A}, σ) be a difference ring and let $\alpha \in \mathbb{A}$. Then we want to decide if we can construct an $R\Pi$ -extension $(\mathbb{A}\langle t \rangle, \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$. First, we have to check if $\alpha \in \mathbb{A}^*$. E.g., for the class of difference rings (\mathbb{A}, σ) , built by simple $R\Pi\Sigma^*$ -extensions introduced in Definition 2.19 below, this task will be straightforward. Next, we need the order of α , i.e., we have to solve the following Problem O with $G := \mathbb{A}^*$.

Problem O in G . Given a group G and $\alpha \in G$. Find $\text{ord}(\alpha)$.

Given $\lambda = \text{ord}(\alpha)$, we can decide which case has to be treated. If $\lambda = 0$, only the construction of a Π -extension might be possible due to Theorem 2.12. Thus we construct the unimonomial extension $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$. Otherwise, if $\lambda > 0$, we construct the algebraic extension $(\mathbb{A}[t], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ of order λ . Finally, we check if our construction is indeed a Π -extension or R -extension, i.e., if the constants remain unchanged. Using Theorem 2.12 this test can be accomplished by solving

Problem MT in (\mathbb{A}, σ) . Given a difference ring (\mathbb{A}, σ) and $\alpha \in \mathbb{A}^*$ with $\lambda = \text{ord}(\alpha)$. Decide if there are a $g \in \mathbb{A} \setminus \{0\}$ and an $m \in \mathbb{Z} \setminus \{0\}$ for the case $\lambda = 0$ (resp. $m \in \{1, \dots, \lambda - 1\}$ for the case $\lambda > 0$) such that the multiplicative version of the telescoping equation (MT) holds:

$$\sigma(g) = \alpha^m g. \tag{11}$$

More generally, if we are given a tower of algebraic and unimonomial extensions, which model indefinite nested products, Problem MT can be used to check if the construction constitutes a nested $R\Pi$ -extension.

Example 2.13 (Cont. Ex. 2.9). We will verify that $(\mathbb{Q}(k)[x][y], \sigma)$ is an R -extension of $(\mathbb{Q}(k), \sigma)$. (1) Take $\alpha = -1$ with $\lambda = \text{ord}(\alpha) = 2$. We solve Problem MP by the algorithms presented below: there are no $g \in \mathbb{Q}(k)^*$ and $m \in \{1\}$ with $\sigma(g) = (-1)^m g$. Hence by Theorem² 2.12.(3) $(\mathbb{Q}(k)[x], \sigma)$ is an R -extension of $(\mathbb{Q}(k), \sigma)$.

(2) Now we solve Problem O for $\alpha = -x$ and get $\lambda = \text{ord}(-x) = 2$; see Example 5.4.(2). In addition, solving Problem MP for α shows that there is no $g \in \mathbb{Q}(k)[x] \setminus \{0\}$ with $\sigma(g) = -xg$. Thus by Theorem 2.12.(3) $(\mathbb{Q}(k)[x][y], \sigma)$ forms an R -extension of $(\mathbb{Q}(k)[x], \sigma)$.

Example 2.14. We construct a ring in which the objects in (7) can be represented.

(0) Take the $\Pi\Sigma^*$ -field $(\mathbb{K}(k), \sigma)$ over $\mathbb{K} = \mathbb{Q}(\iota)$ with $\sigma(k) = k + 1$.

(1) Take $\alpha = \iota$. Then solving Problem O provides $\lambda = \text{ord}(\alpha) = 4$. In particular solving the corresponding Problem MP proves that there are no $g \in \mathbb{K}(k)^*$ and $m \in \{1, 2, 3\}$ with (11). Hence by Theorem 2.12.(3) we can construct the R -extension $(\mathbb{K}(k)[x], \sigma)$ of $(\mathbb{K}(k), \sigma)$ with $\sigma(x) = \iota x$. Note that the R -monomial x represents ι^k .

(2) Take $\alpha = xk$. Solving Problem O yields $\lambda = \text{ord}(\alpha) = 0$ and solving Problem MP shows that there are no $g \in \mathbb{K}(k)[x] \setminus \{0\}$ and $m \in \mathbb{Z} \setminus \{0\}$ with (11). With Theorem 2.12.(2) we can construct the Π -extension $(\mathbb{K}(k)[x], \sigma) \leq (\mathbb{K}(k)[x]\langle t \rangle, \sigma)$ with $\sigma(t) = xkt$; here the Π -monomial t represents $\prod_{j=1}^{k-1} j\iota^j$.

2.2.2. Testing and constructing Σ^* -extensions

In order to verify if a unimonomial extension as given in Theorem 2.12.(1) is a Σ^* -extension, it suffices to solve Problem T with $f = \beta$ and to check if there is not a telescoping solution. We illustrate this feature by actually constructing a difference ring in which the summand

$$f(k) = (-1)^{\binom{k+1}{2}} k^2 \sum_{j=1}^k \frac{(-1)^j}{j} \quad (12)$$

given on the left hand side of (6) and the additional sum

$$\sum_{j=1}^k \frac{(-1)^{\binom{j+1}{2}}}{j} \quad (13)$$

occurring on the right hand side of (6) can be represented. In particular, we demonstrate how identity (6) can be discovered in this difference ring.

Example 2.15 (Cont. Ex. 2.9). (0) Take the difference ring (\mathbb{A}, σ) with $\mathbb{A} = \mathbb{Q}(k)[x][y]$.

(1) Take $f = \sigma(\frac{x}{k}) = \frac{-x}{k+1}$. Then solving Problem T shows that there is no $g \in \mathbb{A}$ with $\sigma(g) - g = \frac{-x}{k+1}$. Hence we can construct the Σ^* -extension $(\mathbb{A}[s], \sigma)$ of (\mathbb{A}, σ) with $\sigma(s) = s + \frac{-x}{k+1}$; note that the Σ^* -monomial s represents $\sum_{j=1}^k \frac{(-1)^j}{j}$.

(2) Take $f = \sigma(\frac{y}{k}) = \frac{-xy}{k+1}$. Then solving Problem T shows that there is no $g \in \mathbb{A}[s]$ with $\sigma(g) - g = \frac{-xy}{k+1}$. Hence we can construct the Σ^* -extension $(\mathbb{A}[s][S], \sigma)$ of $(\mathbb{A}[s], \sigma)$ with $\sigma(S) = S + \frac{-xy}{k+1}$; note that the Σ^* -monomial S represents the sum (13).

(3) Take $f = yk^2s$ which represents (12). Solving Problem T produces the solution

$$g = sy\left(\frac{1}{2}(k-1)(k+1)x - \frac{1}{2}(k-2)k\right) + y\left(\frac{1}{4}(1-2k) - \frac{1}{4}x\right) + \frac{1}{2}S; \quad (14)$$

² Note: Theorem 2.12.(3) is a shortcut for “part 3 of Theorem 2.12”. The same convention will be applied for other references.

for further details see Example 7.3. Hence this yields the solution of the telescoping equation (1) for our summand (12) by replacing the $R\Sigma^*$ -monomials x, y, s, S with the corresponding summation objects. Taking $a = 1$ in (2) and performing the evaluation $c := g(1) = 0 \in \mathbb{Q}$ gives the identity (6).

(4) Note that we succeeded in representing the sum $F(k) = \sum_{i=1}^k f(i)$ with f from (12) in the difference ring in $\mathbb{A}[s][S]$ with $\sigma(g) - c = \sigma(g)$. Namely, replacing the variables in $\sigma(g)$ with the corresponding summation objects yields the right hand side of (6). This is of particular interest if there are further sums defined over $F(k)$ which one wants to represent in a Σ^* -extension over $(\mathbb{A}[s][S], \sigma)$.

We remark that for the derivation of the identity (6) it is crucial to introduce the extra sum (13). Here this was accomplished manually. But, using algorithms from [53,59] in combination with the results of this article, this sum can be determined automatically.

2.2.3. The underlying problems for $R\Pi\Sigma^*$ -extensions

As in the difference field approach [24,49,53,59], Problem T and more generally Problem PT will be solved by reducing them from (\mathbb{A}, σ) to smaller difference rings (i.e., rings built by less $R\Pi\Sigma^*$ -monomials). Likewise, this reduction technique can be applied in order to solve a special case of Problem MT that will cover all the cases needed for our difference ring constructions. However, in order to carry out these reductions, one has to tackle generalized problems within the recursion steps.

For Problem MT the following generalization is needed. Let (\mathbb{A}, σ) be a difference ring, let $W \subseteq \mathbb{A}$ and let $\mathbf{f} = (f_1, \dots, f_n) \in (\mathbb{A}^*)^n$. Then we define the set [24]

$$M(\mathbf{f}, W) := \{(m_1, \dots, m_n) \in \mathbb{Z}^n \mid \sigma(g) = f_1^{m_1} \dots f_n^{m_n} g \text{ for some } g \in W \setminus \{0\}\}.$$

In the following, we want to calculate a finite representation of $M(\mathbf{f}, \mathbb{A})$. If \mathbb{A} is a field, i.e., $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$, it is immediate that $M(\mathbf{f}, \mathbb{A})$ is a submodule of \mathbb{Z}^n over \mathbb{Z} and there is a basis of $M(\mathbf{f}, \mathbb{A})$ with rank $\leq n$; see [24]. In the setting of rings, this result carries over if the set of semi-constants (also called semi-invariants [14]) of (\mathbb{A}, σ) defined by

$$\text{sconst}(\mathbb{A}, \sigma) = \{c \in \mathbb{A} \mid \sigma(c) = u c \text{ for some } u \in \mathbb{A}^*\}$$

forms a multiplicative group (excluding the 0 element). Note: if \mathbb{A} is a field, we have that $\text{sconst}(\mathbb{A}, \sigma) \setminus \{0\} = \mathbb{A} \setminus \{0\} = \mathbb{A}^*$. Unfortunately, for a general difference ring the set $\text{sconst}(\mathbb{A}, \sigma) \setminus \{0\}$ is only a multiplicative monoid [14]. In order to gain more flexibility, we introduce the following refinement. For a given multiplicative subgroup G of \mathbb{A}^* (in short $G \leq \mathbb{A}^*$), we define the set of semi-constants (semi-invariants) of (\mathbb{A}, σ) over G by

$$\text{sconst}_G(\mathbb{A}, \sigma) = \{c \in \mathbb{A} \mid \sigma(c) = u c \text{ for some } u \in G\}.$$

Note that $\text{sconst}_{(\mathbb{A}^*)}(\mathbb{A}, \sigma) = \text{sconst}(\mathbb{A}, \sigma)$ and $\text{sconst}_{\{1\}}(\mathbb{A}, \sigma) = \text{const}(\mathbb{A}, \sigma)$. If it is clear from the context, we drop σ and just write $\text{sconst}_G \mathbb{A}$ and $\text{sconst} \mathbb{A}$, respectively.

Here is one of the main challenges: For all our considerations we will choose G such that $\text{sconst}_G \mathbb{A} \setminus \{0\}$ is a subgroup of \mathbb{A}^* (in short, $\text{sconst} \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$). Then with this careful choice of G we can summarize the above considerations with the following lemma.

Lemma 2.16. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$; let $\mathbf{f} \in G^n$. Then $M(\mathbf{f}, \mathbb{A}) = M(\mathbf{f}, \text{sconst}_G \mathbb{A})$. In particular, $M(\mathbf{f}, \mathbb{A})$ is a submodule of \mathbb{Z}^n over \mathbb{Z} , and it has a finite \mathbb{Z} -basis with rank $\leq n$.

In the light of this property, we can state Problem PMT.

Problem PMT in (\mathbb{A}, σ) for G . *Given a difference ring (\mathbb{A}, σ) with $G \leq \mathbb{A}^*$ such that $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ holds; given $\mathbf{f} \in G^n$. Find a \mathbb{Z} -basis of $M(\mathbf{f}, \mathbb{A})$.*

Observe that Problem MT can be reduced to Problem PMT for a group G with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ if we restrict³ to the situation that $\alpha \in G$. More precisely, assume that we have calculated $\lambda = \text{ord}(\alpha)$ and succeeded in solving Problem PMT, i.e., we are given a basis of $M = M((\alpha), \mathbb{A}) \subseteq \mathbb{Z}^1$. If the basis is empty, there cannot be an $m \in \mathbb{Z} \setminus \{0\}$ and a $g \in \mathbb{A} \setminus \{0\}$ with (11). Otherwise, if the basis is not empty, the rank is 1. More precisely, we obtain $m > 0$ with $M = m\mathbb{Z}$. Hence m is the smallest positive choice such that there is a $g \in \mathbb{A} \setminus \{0\}$ with (11). Therefore we can again decide⁴ Problem MT.

For the generalization of Problems T and PT we introduce the following set. Let (\mathbb{A}, σ) be a difference ring with constant field \mathbb{K} , let $W \subseteq \mathbb{A}$, and let $u \in \mathbb{A} \setminus \{0\}$ and $\mathbf{f} = (f_1, \dots, f_n) \in \mathbb{A}^n$. Then we define [24]

$$V(u, \mathbf{f}, (W, \sigma)) = \{(c_1, \dots, c_n, g) \in \mathbb{K}^n \times W \mid \sigma(g) - u g = c_1 f_1 + \dots + c_n f_n\};$$

if it is clear from the context, we write $V(u, \mathbf{f}, W)$ and suppress the automorphism σ . As with Lemma 2.16 the following result will be crucial for further considerations.

Lemma 2.17. Let (\mathbb{A}, σ) be a difference ring with constant field \mathbb{K} and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let W be a \mathbb{K} -subspace of \mathbb{A} . Then for $\mathbf{f} \in \mathbb{A}^n$ and $u \in G$ we have that $V(u, \mathbf{f}, W)$ is a \mathbb{K} -subspace of $\mathbb{K}^n \times W$ with $\dim V(u, \mathbf{f}, W) \leq n + 1$.

Proof. Suppose that there are m linearly independent solutions with $m > n + 1$, say $(c_{i,1}, \dots, c_{i,n}, g_i)$ with $1 \leq i \leq m$. Then by row operations over the field \mathbb{K} we can derive at least two linearly independent vectors, say $\mathbf{v}_1 = (0, \dots, 0, g)$ and $\mathbf{v}_2 = (0, \dots, 0, h)$. Hence we have that $\sigma(g) = u g$ and $\sigma(h) = u h$ where $g, h \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Consequently, $\sigma(\frac{g}{h}) = \frac{g}{h}$, thus $c = g/h \in \mathbb{K}^*$ and therefore $\mathbf{v}_1 = c \mathbf{v}_2$; a contradiction that the vectors are linearly independent. \square

This result gives rise to the following problem specification.

Problem PFLDE in (\mathbb{A}, σ) for G (with constant field \mathbb{K}). *Given a difference ring (\mathbb{A}, σ) with constant field \mathbb{K} and $G \leq \mathbb{A}^*$ such that $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ holds; given $u \in G$ and $\mathbf{f} \in \mathbb{A}^n$. Find a \mathbb{K} -basis of $V(u, \mathbf{f}, \mathbb{A})$.*

In particular, if we can solve Problem PFLDE in (\mathbb{A}, σ) for G , it follows with $1 \in G$ that we can solve Problem T and PT in (\mathbb{A}, σ) . Furthermore, we can solve the multiplicative version of telescoping: if $\alpha \in G$, we can determine a $g \in \mathbb{A} \setminus \{0\}$, in case of existence, such that $\sigma(g) = \alpha g$ holds. This feature is illustrated by the following example.

³ Note that this restriction, in particular the choice of G , is fundamental: it is the essential step to specify the type of products that one can handle algorithmically; see Definition 2.19.

⁴ Note: If $\lambda := \text{ord}(\alpha) > 0$, we have that $\lambda \in M$, i.e., the rank of M is 1. In particular, we can construct an R -extension $(\mathbb{A}, \sigma) \leq (\mathbb{A}[t], \sigma)$ with $\sigma(t) = \alpha t$ iff $\lambda = m > 0$.

Example 2.18 (Cont. Ex. 2.14). Given $Q(b) = \prod_{k=1}^b \frac{-\iota^k}{1+k}$ on the left hand side of (7), we want to rewrite it in terms of the product $P(b) = \prod_{j=1}^{b-1} j \iota^j$. In a preparation step we constructed already the $R\Pi\Sigma^*$ -extension $(\mathbb{K}(k)[x]\langle t \rangle, \sigma)$ of $(\mathbb{K}(k), \sigma)$ with $\mathbb{K} = \mathbb{Q}(\iota)$, $\sigma(x) = \iota x$ and $\sigma(t) = kxt$ in Example 2.14. There we can represent $\frac{-\iota^k}{k+1}$ with $u = \frac{-x}{k+1}$ and $P(k)$ with t . Now we search for a $g \in \mathbb{K}(k)[x]\langle t \rangle \setminus \{0\}$ such that $\sigma(g) = ug$ holds. More precisely, we are interested in a basis of $V = V(u, (0), \mathbb{K}(k)[x]\langle t \rangle)$. Activating our machinery, we get the basis $\{(0, g), (1, 0)\}$ of V with $g = \frac{x(\iota+x^2)}{k}t^{-1}$. For the chosen group G with $u \in G$, that we use to solve the underlying Problem PFLDE in $(\mathbb{K}(k)[x]\langle t \rangle, \sigma)$, and the corresponding calculation steps we refer to Example 7.6 below. Since g is a solution of $\sigma(g) = ug$, $g(k) = (\iota + (-1)^k) \frac{\iota^k}{k} P(k)^{-1}$ is a solution of $-\frac{\iota^k}{k+1} = \frac{g(k+1)}{g(k)}$. Hence by the telescoping trick we get $\prod_{k=1}^b -\frac{\iota^k}{k+1} = \frac{g(b+1)}{g(1)}$ which produces (7).

2.3. The main results

Suppose that we are given a difference ring (\mathbb{G}, σ) which is computable and we are given a group $G \leq \mathbb{G}^*$ with $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$. In this article we will restrict to certain classes of $R\Pi\Sigma^*$ -extensions (\mathbb{E}, σ) of (\mathbb{G}, σ) equipped with a group \tilde{G} with $G \leq \tilde{G} \leq \mathbb{E}^*$ and $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ such that we can derive the following algorithmic machinery:

- (1) Problem O in \tilde{G} can be reduced to Problem O in G ;
- (2) Problem PMT in (\mathbb{E}, σ) for \tilde{G} can be reduced to Problem PMT in (\mathbb{G}, σ) for G ;
- (3) Problem PFLDE in (\mathbb{E}, σ) for \tilde{G} can be reduced to Problem PFLDE in (\mathbb{G}, σ) for G (see Subsection 2.3.1) or to Problem PFLDE in (\mathbb{G}, σ^k) for G for all $k \geq 1$ (see Subsection 2.3.2).

In a nutshell, if we choose as base case a difference ring (\mathbb{G}, σ) and a group $G \leq \mathbb{G}^*$ in which we can solve Problem O in G and Problems PMT and PFLDE in (\mathbb{G}, σ) for G (resp. (\mathbb{G}, σ^k) for G for all $k \geq 1$), we obtain recursive algorithms that solve the corresponding problems in the larger difference ring (\mathbb{E}, σ) and larger group \tilde{G} .

As it turns out, we will succeed in this task for a subclass of $R\Pi\Sigma^*$ -extensions $(\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)$ and a properly chosen group $\tilde{G} \leq \mathbb{E}^*$ that can treat all objects (among the general class of $R\Pi\Sigma^*$ -extensions) that the author has encountered in practical problem solving so far. More precisely, we will restrict to simple $R\Pi\Sigma^*$ -extensions.

Let $(\mathbb{G}\langle t_1 \rangle \dots \langle t_e \rangle, \sigma)$ be a $R\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) and let $G \leq \mathbb{G}^*$. Then we define

$$G_{\mathbb{G}}^{\mathbb{E}} = \{g t_1^{m_1} \dots t_e^{m_e} \mid h \in G \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^*\text{-monomial}\}. \quad (15)$$

It is easy to see that $\tilde{G} = G_{\mathbb{G}}^{\mathbb{E}}$ forms a group. More precisely, we obtain the following chain of subgroups: $G \leq G_{\mathbb{G}}^{\mathbb{E}} \leq \mathbb{E}^*$. We call $G_{\mathbb{G}}^{\mathbb{E}}$ also the product-group over G for the $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) . We are now ready to define $(G-)$ simple $R\Pi\Sigma^*$ -extensions.

Definition 2.19. Let (\mathbb{G}, σ) be a difference ring and let $G \leq \mathbb{G}^*$ be a group. An $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) with $\mathbb{E} = \mathbb{G}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_e \rangle$ is called G -simple if for any $R\Pi$ -monomial t_i we have that $\sigma(t_i)/t_i \in G_{\mathbb{G}}^{\mathbb{E}}$. Moreover, an $R\Pi$, $R\Sigma^*$, $\Pi\Sigma^*$ -, R -, Π -, and Σ^* -extension of (\mathbb{G}, σ) is G -simple if it is a G -simple $R\Pi\Sigma^*$ -extension. We call any such extension simple if it is \mathbb{G}^* -simple. Analogously, we call an $R\Pi$, $R\Sigma^*$, $\Pi\Sigma^*$ -, R -, Π -, and Σ^* -monomial G -simple (resp. simple) if the extension is G -simple (resp. simple).

In all our examples the difference rings have been built by a simple $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) where (\mathbb{G}, σ) is a $\Pi\Sigma^*$ -field $(\mathbb{K}(k), \sigma)$ over \mathbb{K} with $\sigma(k) = k + 1$. In particular,

the Problems PMT and PFLDE have been considered for the constructed (\mathbb{E}, σ) in $G = (\mathbb{K}(k)^*)^{\mathbb{E}}_{\mathbb{K}(k)}$. Before we finally turn to the class of simple $R\Pi\Sigma^*$ -extensions, we present one example which cannot be treated properly with our toolbox under consideration.

Example 2.20. Take $(\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ from Example 2.5 with $\sigma(k) = k + 1$ and $\sigma(t) = (k + 1)t$. Subsequently, we will use our notation $\mathbb{Q}(k)\langle t \rangle = \mathbb{Q}(k)[t, \frac{1}{t}]$. Then we can construct the R -extension $(\mathbb{Q}(k)\langle t \rangle[x], \sigma)$ of $(\mathbb{Q}(k)\langle t \rangle, \sigma)$ with $\sigma(x) = -x$ of order 2. In this ring we are given the idempotent elements $e_1 = (1 - x)/2$ and $e_2 = (x + 1)/2$ with $e_1^2 = e_1$ and $e_2^2 = e_2$. Finally take $\alpha = e_1 + e_2 t$. Then observe that $\alpha \cdot (e_1 + e_2/t) = 1$, i.e., $\alpha \in \mathbb{Q}(k)\langle t \rangle[x]^*$. Note that $\text{ord}(\alpha) = 0$. Otherwise it would follow that $e_2^\lambda = 0$ with $\lambda = \text{ord}(\alpha) > 0$; a contradiction that e_2 is idempotent. Consequently, T cannot be an R -extension, and we construct the unimonomial extension $(\mathbb{Q}(k)\langle t \rangle[x][T, \frac{1}{T}], \sigma)$ of $(\mathbb{Q}(k)\langle t \rangle[x], \sigma)$ with $\sigma(T) = \alpha T$. It seems non-trivial to derive an (algorithmic) proof (or disproof) that T is a Π -monomial, and it would be nice to see a solution to this problem.

Summarizing, we aim at solving Problems PMT and PFLDE in a G -simple $R\Pi\Sigma^*$ -extension $(\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)$ for $\tilde{G} = G_{\mathbb{G}}^{\mathbb{E}}$, and we want to solve Problem O in \tilde{G} . In order to accomplish this task, we will restrict ourselves further to the following two situations.

2.3.1. A solution for single-rooted $R\Pi\Sigma^*$ -extensions

In most applications R -extensions are not nested, e.g., only objects like $(-1)^k$ arise. In addition, such objects do not occur in transcendental products, but only in sums, like cyclotomic sums [3] or generalized harmonic sums [4]. A formal definition of this special, but very practical oriented class of $R\Pi\Sigma^*$ -extensions is as follows.

Definition 2.21. An $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) is called single-rooted if the generators of the extension can be reordered to

$$\mathbb{E} = \mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle \langle x_1 \rangle \dots \langle x_u \rangle \langle s_1 \rangle \dots \langle s_v \rangle, \quad (16)$$

respecting the recursive nature of the automorphism, such that the t_i are Π -monomials, the x_i are R -monomials with $\sigma(x_i)/x_i \in \mathbb{G}^*$ and the s_i are Σ^* -monomials.

Given this class of single-rooted and simple⁵ $R\Pi\Sigma^*$ -extension, we will show the following theorem in Proof 4.8.

Theorem 2.22. Let (\mathbb{G}, σ) be a difference ring and let $G \leq \mathbb{G}^*$ with $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$. Let (\mathbb{E}, σ) be a simple and single-rooted $R\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) with (16) as specified in Definition 2.21, and let $\tilde{G} = G_{\mathbb{G}}^{\mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle}$. Then $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ with

$$\text{sconst}_{\tilde{G}} \mathbb{E} = \{h t_1^{m_1} \dots t_r^{m_r} x_1^{n_1} \dots x_u^{n_u} \mid h \in \text{sconst}_G \mathbb{G}, m_i \in \mathbb{Z} \text{ and } n_i \in \mathbb{N}\}.$$

In particular, we obtain the following reduction algorithms summarized in Theorem 2.23; for a proof of part 1 see Proof 6.7 and of part 2 see Proof 7.10.

Theorem 2.23. Let (\mathbb{G}, σ) be a computable difference ring with $G \leq \mathbb{G}^*$ and $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$. Let (\mathbb{E}, σ) be a single-rooted and G -simple $R\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) with (16) as given in Definition 2.21, and let $\tilde{G} = G_{\mathbb{G}}^{\mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle}$. Then the following holds.

⁵ Note: If \mathbb{G} is a field, any single-rooted $R\Pi\Sigma^*$ -extension is simple by Corollary 4.15.

- (1) Problem PMT is solvable in (\mathbb{E}, σ) for \tilde{G} if it is solvable in (\mathbb{G}, σ) for G .
- (2) Problem PFLDE is solvable in (\mathbb{E}, σ) for \tilde{G} if Problems PFLDE and PMT are solvable in (\mathbb{G}, σ) for G and if⁶ Problem O is solvable in G .

All the calculations in [44,39,50,33,11,2,1] rely precisely on this machinery. For one of the most important applications we refer to Subsection 2.4.

2.3.2. A solution for simple $R\Pi\Sigma^*$ -extensions of a strong constant-stable difference field

In the following we restrict to simple $R\Pi\Sigma^*$ -extensions where the ground domain $\mathbb{G} = \mathbb{F}$ is a field. In this setting, the semi-constants form a multiplicative group. More precisely, we will show the following result in Proof 4.11.

Theorem 2.24. Let (\mathbb{E}, σ) be a simple $R\Pi\Sigma^*$ -extension of a difference field (\mathbb{F}, σ) and consider its product-group $\tilde{G} = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Then $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$.

For a solution of Problems PMT and PFLDE we require in addition that (\mathbb{F}, σ) is strong constant-stable.

Definition 2.25. A difference ring (\mathbb{A}, σ) with constant field \mathbb{K} is called constant-stable if for all $k > 0$ we have that $\text{const}(\mathbb{A}, \sigma^k) = \mathbb{K}$. It is called strong constant-stable if it is constant-stable and any root of unity of \mathbb{A} is in \mathbb{K} .

In this setting we can treat products over roots of unity from \mathbb{K} and, more generally, products that are built recursively over such products; for examples see (4) and for further (algorithmic) properties see Corollary 5.6 below. More precisely, given such a tower of $R\Pi\Sigma^*$ -extensions, we can solve Problems PMT and PFLDE as follows; for the proofs, resp. the underlying algorithms, of part 1 see Proof 5.7, of part 2 see Proof 6.15 and of part 3 see Proof 7.16.

Theorem 2.26. Let (\mathbb{F}, σ) be a computable difference field where Problem O is solvable in $(\text{const } \mathbb{F})^*$. Let (\mathbb{E}, σ) be a simple $R\Pi\Sigma^*$ -extension of (\mathbb{F}, σ) . Then the following holds.

- (1) Problem O is solvable in $(\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$.

If (\mathbb{F}, σ) is in addition strong constant-stable, then

- (2) Problem PMT is solvable in (\mathbb{E}, σ) for $(\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ if it is solvable in (\mathbb{F}, σ) for \mathbb{F}^* ;
- (3) Problem PFLDE is solvable in (\mathbb{E}, σ) for $(\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ if Problem PMT is solvable in (\mathbb{F}, σ) for \mathbb{F}^* and Problem PFLDE is solvable⁷ in (\mathbb{F}, σ^k) for \mathbb{F}^* for all $k > 0$.

We remark that this reduction machinery has been utilized in Examples 2.15 and 2.18 to obtain the identities (6) and (7), respectively. Further details will be given below.

⁶ Instead of Problem O it suffices if know the orders of all the R -monomials in $(\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)$.

⁷ We emphasize that we will always work with the automorphism σ during the reduction process. Only in the base cases we might face the problem to solve instances of Problem PFLDE in (\mathbb{F}, σ^k) with $k > 1$. In a nutshell, we succeed in avoiding to work with σ^k for some $k > 1$ as much as possible. This strategy is of particular advantage, if (\mathbb{F}, σ) is built only by few summation objects. Then the typical phenomenon of the expression swell in symbolic summation due to σ^k is prevented as much as possible.

2.3.3. A complete machinery: algorithms for the ground difference rings

Both, Theorems 2.23 and 2.26 provide algorithms to reduce the Problems PMT and PFLDE (and thus the Problems T, PT and special cases of Problem MT) from an $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) to the ground difference ring (\mathbb{G}, σ) . Theorem 2.23 requires less conditions on (\mathbb{G}, σ) , but considers only single-rooted $R\Pi\Sigma^*$ -extensions, whereas Theorem 2.26 requires more properties on (\mathbb{G}, σ) but allows nested R -extensions which are of the type as given in Corollary 5.6 below. Note that the algorithms for the latter case are more demanding, in particular, one has to solve Problem PFLDE in (\mathbb{G}, σ^k) with $k > 0$ instead of $k = 1$ only.

We emphasize that both theorems are applicable for a rather general class of difference fields (\mathbb{G}, σ) . Namely, (\mathbb{G}, σ) itself can be a $\Pi\Sigma^*$ -field extension of (\mathbb{H}, σ) where certain properties in the difference field (\mathbb{H}, σ) hold. Here the following remarks are in place.

(a) By [24] a $\Pi\Sigma^*$ -field extension (\mathbb{G}, σ) of (\mathbb{H}, σ) is constant-stable if (\mathbb{H}, σ) is constant-stable. In particular, if we are given a root of unity from \mathbb{G} , it cannot depend on transcendental elements and is therefore from \mathbb{H} . Thus (\mathbb{G}, σ) is strong constant-stable if (\mathbb{H}, σ) is strong constant-stable.

(b) It has been shown in [28] that one can solve Problem PMT in (\mathbb{G}, σ) for \mathbb{G}^* and Problem PFLDE in (\mathbb{G}, σ^k) for \mathbb{G}^* for $k > 0$ if certain properties hold for the difference field (\mathbb{H}, σ) . Among others (see Def. 1 and 2 in [28]) Problem PMT must be solvable in (\mathbb{H}, σ) for \mathbb{H}^* and Problem PFLDE must be solvable in (\mathbb{H}, σ^k) for \mathbb{H}^* .

Summarizing, if we are given the tower of extensions

$$(\mathbb{H}, \sigma) \xrightarrow{\Pi\Sigma^*\text{-field ext.}} (\mathbb{G}, \sigma) \xrightarrow{R\Pi\Sigma^*\text{-ring ext.}} (\mathbb{E}, \sigma)$$

where (\mathbb{H}, σ) is strong constant-stable and the properties given in Def. 1 and 2 of [28] hold in (\mathbb{H}, σ) , then we can solve Problems PMT and PFLDE in (\mathbb{E}, σ) for $(\mathbb{G}^*)_{\mathbb{G}}^{\mathbb{E}}$.

So far, the required properties have been verified and the necessary algorithms have been worked out for the following difference fields (\mathbb{H}, σ) with constant field \mathbb{K} .

- (1) $\mathbb{K} = \mathbb{H}$, i.e., (\mathbb{G}, σ) is a $\Pi\Sigma^*$ -field over \mathbb{K} ; here the constant field \mathbb{K} can be a rational function field over an algebraic number field; see [48, Theorem 3.5].
- (2) (\mathbb{H}, σ) is a free difference field, i.e., $\mathbb{H} = \mathbb{K}(\dots, x_{-1}, x_0, x_1, \dots)$ with $\sigma(x_i) = x_{i+1}$; here \mathbb{K} is of the type as given in case (1). Note that in this field one can model unspecified sequences; see [28, 27].
- (3) (\mathbb{H}, σ) can be a radical difference field representing objects like $\sqrt[d]{k}$; see [29].

For simplicity, all our examples are chosen from case (1). More precisely, we always take the $\Pi\Sigma^*$ -field $(\mathbb{H}, \sigma) = (\mathbb{K}(k), \sigma)$ over $\mathbb{K} \in \{\mathbb{Q}, \mathbb{Q}(\iota)\}$ with $\sigma(k) = k + 1$.

2.4. Application: representation of d'Alembertian solutions in $R\Pi\Sigma^*$ -extensions

We illustrate how an important class of d'Alembertian solutions [7], a subclass of Liouvillian solutions [20, 38], of a given linear difference operator, can be represented completely automatically in $R\Pi\Sigma^*$ -extensions. In order to obtain the d'Alembertian solutions, one starts as follows: first the linear difference operator is factored as much as possible into linear right hand factors. This can be accomplished, e.g., with the algorithms from [36, 21, 22] or, within the setting of $\Pi\Sigma^*$ -fields with the algorithms given in [6] which are based on [14, 42, 49]. The latter machinery is available within the summation package **Sigma**. Then given this factored form of the operator, the d'Alembertian solutions can be read off. They can be given by a finite number of hypergeometric expressions and

indefinite nested sums defined over such expressions. More precisely, each solution is of the form

$$\sum_{i_1=\lambda_1}^k h_1(i_1) \sum_{i_2=\lambda_2}^{i_1} h_2(i_2) \cdots \sum_{i_r=\lambda_{r-1}}^{i_{r-1}} h_r(i_r) \quad (17)$$

where $\lambda_i \in \mathbb{N}$ and the hypergeometric expression $h_i(k)$ can be written in the form $\prod_{j=\lambda_i}^k \alpha_i(j)$ with $\alpha_i(z)$ being a rational function from $\mathbb{K}(z)$.

Subsequently, we restrict ourselves to a field \mathbb{K} which is a rational function field $\mathbb{K} = \mathbb{Q}(n_1, \dots, n_r)$ over the rational numbers. Now take the $\Pi\Sigma^*$ -field $(\mathbb{K}(k), \sigma)$ over \mathbb{K} with $\sigma(k) = k + 1$. Then the solutions, all being of the form (17), can be represented in a single-rooted simple $R\Pi\Sigma^*$ -extension as follows.

(1) In [48, Section 6] an algorithm has been presented that calculates a single-rooted simple $R\Pi$ -extension (\mathbb{G}, σ) of $(\mathbb{K}(k), \sigma)$ in which all hypergeometric expressions occurring in the d'Alembertian solutions are explicitly represented.

(2) Then the challenging task is to construct a Σ^* -extension of (\mathbb{G}, σ) and to represent there the arising sums of the d'Alembertian solutions. Given (\mathbb{G}, σ) from step 1, this can be accomplished by applying iteratively Theorem 2.12.(1). Suppose we represented already an inner summand in a Σ^* -extension (\mathbb{A}, σ) of (\mathbb{G}, σ) with $\beta \in \mathbb{A}$. Since (\mathbb{A}, σ) is a simple $R\Pi\Sigma^*$ -extension of $(\mathbb{K}(k), \sigma)$ and $(\mathbb{K}(k), \sigma)$ is a $\Pi\Sigma^*$ -field over \mathbb{K} , we can solve Problem T with $f = \beta$ by using the underlying algorithm of Theorem 2.23 in combination with the base case algorithms; see Subsection 2.3.3. If we find a $g \in \mathbb{A}$ with $\sigma(g) = g + \beta$, we can represent the sum under consideration with $g + c$ where $c \in \mathbb{K}$ is determined by the boundary condition (lower summation bound) of the given sum; for further details we refer to Example 2.15.(4). Otherwise, we construct the Σ^* -extension $(\mathbb{A}[t], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = t + \beta$ by Theorem 2.12.(1) and we succeeded in representing the sum under consideration by t with the appropriate shift behaviour. Note that $(\mathbb{A}[t], \sigma)$ is again a single-rooted simple $R\Pi\Sigma^*$ -extension of $(\mathbb{K}(k), \sigma)$. Proceeding iteratively, all the nested hypergeometric sums are represented in terms of an $R\Pi\Sigma^*$ -extension over $(\mathbb{K}(k), \sigma)$.

Exactly this difference ring machinery is implemented in **Sigma** and has been used to tackle challenging applications, like [44,39,50,33,11,2,1] mentioned already in the introduction. In particular, this toolbox has been combined with the algorithms worked out in [45,48,51,53,8,59] in order to find representations of d'Alembertian solutions with certain optimality properties, like minimal nesting depth. For a recent summary of all these features (unfortunately, in the setting of difference fields) we refer to [57,58].

3. Single nested $R\Pi\Sigma^*$ -extensions

This section delivers relevant properties of single nested $R\Pi\Sigma^*$ -extensions. The characterization of $R\Pi\Sigma^*$ -extensions (Theorem 2.12) will be elaborated. In addition, properties of the semi-constants within $R\Pi\Sigma^*$ -extensions are derived to gain further insight in the nature of $R\Pi\Sigma^*$ -extensions and to prove Theorems 2.22 and 2.24 in Section 4.

We start with some general properties which will be essential throughout this article.

Definition 3.1. A ring \mathbb{A} is called reduced if there are no non-zero nilpotent elements, i.e., for any $f \in \mathbb{A} \setminus \{0\}$ and any $n > 0$ we have that $f^n \neq 0$. \mathbb{A} is called connected if 0 and 1 are the only idempotent elements, i.e., for any $f \in \mathbb{A} \setminus \{0, 1\}$ we have that $f^2 \neq f$.

Namely, we rely on the following ring properties. A polynomial $\sum_{i=0}^n a_i x^i \in \mathbb{A}[t]$ with coefficients from a ring \mathbb{A} is invertible if and only if $a_0 \in \mathbb{A}^*$ and a_i with $i \geq 1$ are nilpotent elements. Thus in a reduced ring, i.e., a ring which has no nilpotent non-zero elements, we have that $\mathbb{A}[t]^* = \mathbb{A}^*$. Besides, there is a complete characterization of invertible elements in the ring of Laurent polynomials $\mathbb{A}[t, \frac{1}{t}]$ presented in [23, Theorem 1] (see also [32]). Based on this work we extract the following crucial result.

Lemma 3.2. Let \mathbb{A} be a commutative ring with 1. If \mathbb{A} is reduced, then $\mathbb{A}[t]^* = \mathbb{A}^*$. If \mathbb{A} is reduced and connected, then $\mathbb{A}[t, \frac{1}{t}]^* = \{u t^r \mid u \in \mathbb{A}^* \text{ and } r \in \mathbb{Z}\}$.

Since our rings are usually not connected, Lemma 3.2 can be applied only partially.

Example 3.3. The generators in the ring given in Example 2.20 can be reordered to $\mathbb{Q}(k)[x]\langle t \rangle$. Since $\mathbb{Q}(k)[x]$ has the idempotent elements e_1, e_2 , it is not connected. Therefore we get relations such as $(e_1 + e_2 t)(e_1 + \frac{e_2}{t}) = 1$ which are predicted in [23,32].

Subsequently, we enumerate further definitions and properties in difference rings and fields that will be used throughout the article. Let (\mathbb{A}, σ) be a difference ring. The rising factorial (or σ -factorial) of $f \in \mathbb{A}^*$ to $k \in \mathbb{Z}$ is defined by

$$f_{(k, \sigma)} = \begin{cases} f \sigma(f) \dots \sigma^{k-1}(f) & \text{if } k > 0 \\ 1 & \text{if } k = 0 \\ \sigma^{-1}(f^{-1}) \sigma^{-2}(f^{-1}) \dots \sigma^k(f^{-1}) & \text{if } k < 0. \end{cases}$$

If the automorphism is clear from the context, we also will write $f_{(k)}$ instead of $f_{(k, \sigma)}$. We will rely on the following simple identities (compare also [25, page 307]). The proofs are omitted to the reader.

Lemma 3.4. Let (\mathbb{A}, σ) be a difference ring, $f, h \in \mathbb{A}^*$ and $n, m \in \mathbb{Z}$. Then:

- (1) $(f h)_{(n)} = f_{(n)} h_{(n)}$.
- (2) $f_{(n+m)} = \sigma^n(f_{(m)}) f_{(n)}$.
- (3) $f_{(n m)} = (f_{(n, \sigma)})_{(m, \sigma^n)}$.
- (4) If $\sigma(h) = f h$, then $\sigma^n(h) = f_{(n)} h$.
- (5) $\sigma^k(f) \in \mathbb{A}^*$ and $f_{(n)} \in \mathbb{A}^*$.

Let $\mathbb{A}\langle t \rangle$ be a ring of (Laurent) polynomials. For $f = \sum_i f_i t^i \in \mathbb{A}\langle t \rangle$ we define

$$\deg(f) = \begin{cases} \max\{i \mid f_i \neq 0\} & \text{if } f \neq 0 \\ -\infty & \text{if } f = 0 \end{cases} \quad \text{and} \quad \text{ldeg}(f) = \begin{cases} \min\{i \mid f_i \neq 0\} & \text{if } f \neq 0 \\ \infty & \text{if } f = 0. \end{cases}$$

In addition, for $a, b \in \mathbb{Z}$ we introduce the set of truncated (Laurent) polynomials by

$$\mathbb{A}\langle t \rangle_{a, b} = \left\{ \sum_{i=a}^b f_i t^i \mid f_i \in \mathbb{A} \right\}. \quad (18)$$

We conclude this part with the following two lemmas.

Lemma 3.5. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) of (Laurent) polynomial type. Then for any $k \in \mathbb{Z}$ and $f \in \mathbb{A}\langle t \rangle$ we have that $\deg(\sigma^k(f)) = \deg(f)$.

Proof. Let $f = \sum_i f_i t_i$. If $f = 0$, $\sigma^k(f) = 0$ and thus with $\deg(0) = -\infty$ the statement holds. Otherwise, let $m := \deg(f) \in \mathbb{Z}$. Then note that $\sigma^k(f) = \sum_i \sigma^k(f_i)(\sigma^k(t))^i$, i.e., t^m is the largest possible monomial in $\sigma^k(f)$ with the coefficient $h := \alpha_{(k)}^m \sigma^k(f_m)$. Since $\sigma^k(f_m) \neq 0$ and $\alpha_{(k)} \in \mathbb{A}^*$ by Lemma 3.4.(5), the coefficient h is non-zero. \square

Lemma 3.6. Let $(\mathbb{F}(t), \sigma)$ be a unimonomial field extension of (\mathbb{F}, σ) , and let $p, q \in \mathbb{F}[t]^*$ with $\gcd(p, q) = 1$ and $k \in \mathbb{Z}$. Then the following holds.

- (1) If $p \mid q$ then $\sigma^k(p) \mid \sigma^k(q)$.
- (2) $\gcd(\sigma^k(p), \sigma^k(q)) = 1$.
- (3) $\frac{\sigma(p/q)}{p/q} \in \mathbb{F}$ if and only if $\sigma(p)/p \in \mathbb{F}$ and $\sigma(q)/q \in \mathbb{F}$.

Proof. (1) If $p \mid q$, i.e., $p w = q$ for some $w \in \mathbb{F}[t] \setminus \{0\}$, then $\sigma^k(p) = \sigma^k(w) \sigma^k(q)$, and thus $\sigma^k(p) \mid \sigma^k(q)$. (2) Suppose that $1 \neq \gcd(\sigma^k(p), \sigma^k(q)) =: u \in \mathbb{F}[t] \setminus \mathbb{F}$. Then $\sigma^{-k}(u) \in \mathbb{F}[t] \setminus \mathbb{F}$. Since $\sigma^{-k}(u) \mid p$ and $\sigma^{-k}(u) \mid q$ by part 1 of the lemma, $\gcd(p, q) \neq 1$, a contradiction to the assumption. (3) The implication \Leftarrow is immediate. Suppose that $u := \sigma(p/q)/(p/q) \in \mathbb{F}$, i.e., $\sigma(p)q = u p \sigma(q)$. By part 2 of the lemma, $\sigma(p) \mid p$ and $p \mid \sigma(p)$ which implies that $\sigma(p)/p \in \mathbb{F}$. Analogously, it follows that $\sigma(q)/q \in \mathbb{F}$. \square

3.1. Σ^* -extensions

The essence of all the properties of Σ^* -extensions is contained in the following lemma.

Lemma 3.7. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t], \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) with $\sigma(t) = t + \beta$ for some $\beta \in \mathbb{A}$. If there are a $u \in G$ and a $g \in \mathbb{A}[t]$ with $\deg(g) \geq 1$ such that

$$\deg(\sigma(g) - u g) < \deg(g) - 1 \quad (19)$$

holds, then there is a $\gamma \in \mathbb{A}$ with $\sigma(\gamma) - \gamma = \beta$.

Proof. Let $g = \sum_{i=0}^n g_i t^i \in \mathbb{A}[t]$ with $\deg(g) = n \geq 1$ and $u \in G$ as stated in the lemma, and define $f = \sigma(g) - u g \in \mathbb{A}[t]$. With (19) it follows that $f = \sum_{i=0}^{n-2} f_i t^i$. Thus comparing the n th and $(n-1)$ th coefficient in $\sum_{i=0}^{n-2} f_i t^i = f = \sigma(g) - u g = \sum_{i=0}^n \sigma(g_i)(t + \beta)^i - u \sum_{i=0}^n g_i t^i$ and using $(t + \beta)^i = \sum_{j=0}^i \binom{i}{j} t^{i-j} \beta^j$ for $0 \leq i \leq n$ yield

$$\sigma(g_n) - u g_n = 0 \quad \text{and} \quad \sigma(g_{n-1}) + \sigma(g_n) \binom{n}{1} \beta - u g_{n-1} = 0.$$

The first equation shows that $g_n \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Hence we get $u = \sigma(g_n)/g_n$. Substituting u for $\sigma(g_n)/g_n$ in the second equation gives $\sigma(g_{n-1}) - \frac{\sigma(g_n)}{g_n} g_{n-1} = -n \beta \sigma(g_n)$. Dividing this equation by $-n \sigma(g_n) \in \mathbb{A}^*$ yields $\sigma(\gamma) - \gamma = \beta$ with $\gamma := \frac{-g_{n-1}}{n g_n} \in \mathbb{A}$. \square

Lemma 3.7 leads to the following equivalent properties of Σ^* -extensions.

Lemma 3.8. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t], \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) with $\sigma(t) = t + \beta$ for some $\beta \in \mathbb{A}$. Then the following statements are equivalent.

- (1) There is a $g \in \mathbb{A}[t] \setminus \mathbb{A}$ and $u \in G$ with $\sigma(g) = u g$.
- (2) There is a $g \in \mathbb{A}$ with $\sigma(g) = g + \beta$.
- (3) $\text{const} \mathbb{A}[t] \supsetneq \text{const} \mathbb{A}$.

Proof. (1) \Rightarrow (2): Let $g \in \mathbb{A}[t] \setminus \mathbb{A}$, $u \in G$ with $\sigma(g) = ug$. Since $\deg(g) \geq 1$ and $\deg(\sigma(g) - ug) < 0 \leq \deg(g) - 1$, there is a $\gamma \in \mathbb{A}$ with $\sigma(\gamma) = \gamma + \beta$ by Lemma 3.7.
(2) \Rightarrow (3): Let $g \in \mathbb{A}$ with $\sigma(g) = g + \beta$. Since $\sigma(t) = t + \beta$, it follows that $\sigma(t - g) = (t - g)$, i.e., $t - g \in \text{const } \mathbb{A}[t]$. Since $t - g \notin \mathbb{A}$, $t - g \notin \text{const } \mathbb{A}$.
(3) \Rightarrow (1): Suppose that $\text{const } \mathbb{A} \subsetneq \text{const } \mathbb{A}[t]$ and take $g \in \text{const } \mathbb{A}[t] \setminus \text{const } \mathbb{A}$. Then $\sigma(g) = ug$ with $u = 1 \in G$. Thus the lemma is proven. \square

As a consequence we can now establish the characterization theorem of Σ^* -extensions.

Proof 3.9. (Theorem 2.12.(1)). For $G = \{1\}$ we have that $\text{sconst}_G \mathbb{A} = \text{const } \mathbb{A} = \mathbb{K}$. By assumption \mathbb{K} is a field and thus $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Therefore we can apply Lemma 3.8 and its equivalence (2) \Leftrightarrow (3) establishes Theorem 2.12.(1). \square

In order to rediscover the difference field version from [24,25], we specialize Lemma 3.8 to difference fields by exploiting Lemma 3.6.(3).

Lemma 3.10. Let $(\mathbb{F}(t), \sigma)$ be a unimonomial field extension of (\mathbb{F}, σ) with $\sigma(t) = t + \beta$ for some $\beta \in \mathbb{F}$. Then the following statements are equivalent.

- (1) There is a $g \in \mathbb{F}(t) \setminus \mathbb{F}$ with $\frac{\sigma(g)}{g} \in \mathbb{F}$.
- (2) There is a $g \in \mathbb{F}$ with $\sigma(g) = g + \beta$.
- (3) $\text{const } \mathbb{F}(t) \supsetneq \text{const } \mathbb{F}$.

Proof. (1) \Rightarrow (2): Let $g \in \mathbb{F}(t) \setminus \mathbb{F}$ with $\sigma(g)/g \in \mathbb{F}$. Write $g = \frac{p}{q}$ with $p, q \in \mathbb{F}[t]^*$ and $\gcd(p, q) = 1$. By Lemma 3.6, $\sigma(p)/p \in \mathbb{F}$ and $\sigma(q)/q \in \mathbb{F}$. Since $g \notin \mathbb{F}$, we have that $p \notin \mathbb{F}$ or $q \notin \mathbb{F}$. Thus there is a $g' \in \mathbb{F}[t]$ with $\deg(g') \geq 1$ and $\deg(\sigma(g') - g') = \deg(0) = -\infty < 0 \leq \deg(g') - 1$. Hence by Lemma 3.7 there is a $\gamma \in \mathbb{F}$ with $\sigma(\gamma) = \gamma + \beta$.
(2) \Rightarrow (3) follows by Lemma 3.8. (3) \Rightarrow (1) is analogous to the proof of Lemma 3.8. \square

Note that the above lemma is contained in Karr's work by combining Theorems 2.1 and 2.3 from [25]. As a consequence, we obtain the following result.

Theorem 3.11. Let $(\mathbb{F}(t), \sigma)$ be a unimonomial field extension of (\mathbb{F}, σ) with $\sigma(t) = t + \beta$ for some $\beta \in \mathbb{F}$. Then this is a Σ^* -extension iff there is no $g \in \mathbb{F}$ with $\sigma(g) = g + \beta$.

By the equivalence (3) \Leftrightarrow (1) of Lemma 3.8 we obtain the following result concerning the semi-constants.

Theorem 3.12. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. If $(\mathbb{A}[t], \sigma)$ is a Σ^* -extension of (\mathbb{A}, σ) , then $\text{sconst}_G \mathbb{A}[t] = \text{sconst}_G \mathbb{A}$.

Furthermore, if we specialize to $G = \mathbb{A}[t]^*$ and assume that \mathbb{A} is reduced, we get Theorem 3.14. For its proof given below we use in addition the following lemma.

Lemma 3.13. Let (\mathbb{A}, σ) be a difference ring: $\text{sconst } \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ iff $\text{sconst } \mathbb{A} \setminus \{0\} = \mathbb{A}^*$.

Proof. Suppose that $\text{sconst } \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. If $a \in \mathbb{A}^*$, then $\sigma(a) \in \mathbb{A}^*$. Thus $u := \frac{\sigma(a)}{a} \in \mathbb{A}^*$. With $\sigma(a) = ua$ it follows that $a \in \text{sconst } \mathbb{A} \setminus \{0\}$. Hence $\text{sconst } \mathbb{A} \setminus \{0\} \supseteq \mathbb{A}^*$ and with $\text{sconst } \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ we have $\text{sconst } \mathbb{A} \setminus \{0\} \subseteq \mathbb{A}^*$. The other implication is immediate. \square

Theorem 3.14. Let $(\mathbb{A}[t], \sigma)$ be a Σ^* -extension of (\mathbb{A}, σ) where \mathbb{A} is reduced and $\text{sconst } \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Then $\text{sconst } \mathbb{A}[t] \setminus \{0\} = \text{sconst } \mathbb{A} \setminus \{0\} = \mathbb{A}^*$.

Proof. By Lemma 3.13 it follows that $\text{sconst}\mathbb{A} \setminus \{0\} = \mathbb{A}^*$. Since \mathbb{A} is reduced, $\mathbb{A}[t]^* = \mathbb{A}^*$ by Lemma 3.2 and thus $\text{sconst}\mathbb{A}[t] = \text{sconst}_{\mathbb{A}[t]^*}\mathbb{A}[t] = \text{sconst}_{\mathbb{A}^*}\mathbb{A}[t]$. Now take $G = \mathbb{A}^*$ and apply Theorem 3.12. Hence $\text{sconst}_{\mathbb{A}^*}\mathbb{A}[t] = \text{sconst}_{\mathbb{A}^*}\mathbb{A} = \text{sconst}\mathbb{A}$. \square

3.2. Π -extensions

Analogously to Lemma 3.7 we obtain by coefficient comparison the following lemma.

Lemma 3.15. Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be a unimonomial ring extension of (\mathbb{A}, σ) with $\alpha = \frac{\sigma(t)}{t} \in \mathbb{A}^*$; let $u \in \mathbb{A}$ and $g = \sum_{i=0}^n g_i t^i \in \mathbb{A}[t, \frac{1}{t}]$. If $\sigma(g) = u g$, then $\sigma(g_i) = u \alpha^{-i} g_i$ for all i .

Now we are in the position to obtain the characterization theorem of Π -extensions.

Proof 3.16. (Theorem 2.12.(2)). “ \Leftarrow ”: Let $m \in \mathbb{Z} \setminus \{0\}$ and $g \in \mathbb{A} \setminus \{0\}$ with $\sigma(g) = \alpha^m g$. Since $\sigma(t^m) = \alpha^m t^m$, it follows that $\sigma(g/t^m) = g/t^m$, i.e., $g/t^m \in \text{const}\mathbb{A}[t, \frac{1}{t}]$. Clearly $g/t^m \notin \mathbb{A}$ which implies that $g/t^m \notin \text{const}\mathbb{A}$.

“ \Rightarrow ”: Let $g = \sum_i g_i t^i \in \mathbb{A}[t, \frac{1}{t}] \setminus \mathbb{A}$ such that $\sigma(g) = g$. Thus $g_m \neq 0$ for some $m \neq 0$. By Lemma 3.15 we have that $\sigma(g_m) = \alpha^{-m} g_m$.

Suppose that t is a Π -monomial, but $\text{ord}(\alpha) = n > 0$. Then $\sigma(t^n) = \alpha^n t^n = t^n$, which is a contradiction to the first part of the statement. \square

Requiring in addition that the semi-constants form a group, this result can be sharpened.

Theorem 3.17. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be a unimonomial extension of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ for some $\alpha \in G$. Then this is a Π -extension iff there are no $g \in \text{sconst}_G \mathbb{A} \setminus \{0\}$ and $m > 0$ with $\sigma(g) = \alpha^m g$.

Proof. \Rightarrow : Suppose that t is not a Π -monomial. Then we can take $g \in \mathbb{A} \setminus \{0\}$ and $m \in \mathbb{Z} \setminus \{0\}$ with $\sigma(g) = \alpha^m g$. Hence $g \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Thus if $m < 0$, we get $\sigma(\tilde{g}) = \alpha^{-m} \tilde{g}$ with $\tilde{g} = \frac{1}{g} \in \mathbb{A}^*$. The other direction is immediate by Theorem 2.12.(2). \square

Together with Lemma 3.6 we rediscover Karr’s field version; see [25, Theorem 2.2]

Theorem 3.18. Let $(\mathbb{F}(t), \sigma)$ be a unimonomial field extension of (\mathbb{F}, σ) with $\alpha = \frac{\sigma(t)}{t} \in \mathbb{F}^*$. Then this is a Π -extension iff there are no $g \in \mathbb{F}^*$ and $m > 0$ with $\sigma(g) = \alpha^m g$.

Proof. The direction from right to left follows by Theorem 2.12.(2) and the fact that any Π -field extension is a Π -ring extension. Now let $g \in \mathbb{F}(t) \setminus \mathbb{F}$ with $\sigma(g) = g$. Write $g = p/q$ with $p, q \in \mathbb{F}(t)$ where $\gcd(p, q) = 1$ and q is monic. W.l.o.g. suppose that $\deg(q) \geq \deg(p)$ (otherwise take $1/g$ instead of g). By Lemma 3.6,

$$\sigma(p)/p \in \mathbb{F} \quad \text{and} \quad \sigma(q)/q \in \mathbb{F}. \quad (20)$$

We consider two cases. First suppose that $p \in \mathbb{F}^*$ and $q = t^m$ with $m > 0$. Then $\frac{p}{t^m} = g = \sigma(g) = \frac{\sigma(p)}{\alpha^m t^m}$ which implies that $\sigma(p) = \alpha^m p$. What remains to consider is the case that $p \notin \mathbb{F}$ or $q \neq t^m$ for some $m > 0$. Define

$$a := \begin{cases} p & \text{if } q = t^m \text{ for some } m > 0, \\ q & \text{otherwise.} \end{cases}$$

The following holds.

- (1) $a \in \mathbb{F}[t] \setminus \mathbb{F}$: If $a = q$, note that $q \notin \mathbb{F}$ by $\deg(p) \leq \deg(q)$ and $p/q \notin \mathbb{F}$; if $a = p$, $q = t^m$ and hence $p \notin \mathbb{F}$ by assumption.
- (2) $u := \sigma(a)/a \in \mathbb{F}^*$ by (20).
- (3) $a \neq ut^m$ for all $u \in \mathbb{F}^*$ and $m > 0$: a could be only of this form, if $q = t^m$ for some $m > 0$. Hence $a = p$. But since $\gcd(p, q) = 1$, $t \nmid p$.

By the properties (1) and (3), it follows that $a = \sum_{i=k}^n a_i t^i$ with $a_k \neq 0 \neq a_n$ where $n > k \geq 0$. Property (2) and Lemma 3.15 yield $\sigma(a_k) = \frac{u}{\alpha^k} a_k$ and $\sigma(a_n) = \frac{u}{\alpha^n} a_n$ which implies $\sigma(\frac{a_k}{a_n}) = \alpha^{n-k} \frac{a_k}{a_n}$. Since $\frac{a_k}{a_n} \in \mathbb{F}^*$ and $n - k > 0$, the theorem is proven. \square

Finally, we characterize the set of semi-constants for Π -extensions.

Proposition 3.19. Let (\mathbb{A}, σ) be a difference ring with $G \leq \mathbb{A}^*$ and $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be Π -extension of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ for some $\alpha \in G$. Then $\text{sconst}_G \mathbb{A}[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst}_G \mathbb{A} \text{ and } m \in \mathbb{Z}\}$ and $\text{sconst}_G \mathbb{A}[t, \frac{1}{t}] \setminus \{0\} \leq \mathbb{A}[t, \frac{1}{t}]^*$.

Proof. “ \subseteq ”: Let $g \in \text{sconst}_G \mathbb{A}[t, \frac{1}{t}]$, i.e., $g = \sum_i g_i t^i \in \mathbb{A}[t, \frac{1}{t}]$ with $\sigma(g) = u g$ for some $u \in G$. By Lemma 3.15 we get $\sigma(g_i) \alpha^i = u g_i$ and thus $\sigma(g_i) = \frac{u}{\alpha^i} g_i$. Now suppose that there are $r, s \in \mathbb{Z}$ with $s > r$ and $g_r \neq 0 \neq g_s$. As $\frac{u}{\alpha^s} \in G$, it follows that $g_s \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Thus we conclude that $\sigma(\frac{g_r}{g_s}) = \alpha^{s-r} \frac{g_r}{g_s}$ with $s - r > 0$; a contradiction to Theorem 2.12.(2). Hence $g = h t^m$ for some $h \in \text{sconst}_G \mathbb{A}$, $m \in \mathbb{Z}$.

“ \supseteq ”: Let $g = h t^m$ with $h \in \text{sconst}_G \mathbb{A}$, $m \in \mathbb{Z}$. Then there is a $u \in G$ with $\sigma(h) = u h$. Hence $\sigma(g) = \sigma(h) \alpha^m t^m = u \alpha^m h t^m = u \alpha^m g$ with $u \alpha^m \in G$. Thus $g \in \text{sconst}_G \mathbb{A}[t, \frac{1}{t}]$. Summarizing, we proved equality which implies that $\text{sconst}_G \mathbb{A}[t, \frac{1}{t}] \setminus \{0\} \leq \mathbb{A}[t, \frac{1}{t}]^*$. \square

So far we obtained a description of the semi-constants for a subgroup G of \mathbb{A}^* . Now we will lift this result to the group

$$\tilde{G} = G_{\mathbb{A}}^{\mathbb{A}\langle t \rangle} = \{h t^m | h \in G \text{ and } m \in \mathbb{Z}\} \leq \mathbb{A}\langle t \rangle^*.$$

Theorem 3.20. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be Π -extension of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ for some $\alpha \in G$ and let $\tilde{G} = G_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$. Then $\text{sconst}_{\tilde{G}} \mathbb{A}[t, \frac{1}{t}] = \text{sconst}_G \mathbb{A}[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst}_G \mathbb{A} \text{ and } m \in \mathbb{Z}\}$.

Proof. We show that $\text{sconst}_{\tilde{G}} \mathbb{A}[t, \frac{1}{t}] = \text{sconst}_G \mathbb{A}[t, \frac{1}{t}]$. Then by Proposition 3.19 the theorem is proven. Since $G \leq \tilde{G}$, the inclusion $\text{sconst}_{\tilde{G}} \mathbb{A}[t, \frac{1}{t}] \supseteq \text{sconst}_G \mathbb{A}[t, \frac{1}{t}]$ is immediate. Now suppose that $g = \sum_i g_i t^i \in \text{sconst}_{\tilde{G}} \mathbb{A}[t, \frac{1}{t}]$. Hence there are an $m \in \mathbb{Z}$ and an $h \in G$ with $\sigma(g) = h t^m g$. By coefficient comparison it follows that $\sigma(g_i) \alpha^i = h g_{i-m}$. If $m \geq 1$, take s minimal such that $g_s \neq 0$. Then $\sigma(g_s) \alpha^s \neq 0$. But by the choice of s , we get $g_{s-m} = 0$ and thus $h g_{s-m} = 0$, a contradiction. Otherwise, if $m < 0$, take s maximal such that $g_{s-m} \neq 0$. Then $h g_{s-m} \neq 0$. But by the choice of s , we get $\sigma(g_s) \alpha^s = 0$, again a contradiction. Thus $m = 0$ and consequently, $g \in \text{sconst}_G \mathbb{A}[t, \frac{1}{t}]$. \square

We close this subsection with Theorem 3.21. It provides a description of $\text{sconst} \mathbb{A}[t, \frac{1}{t}]$ under the assumption that \mathbb{A} is reduced and connected. This result is not applicable if general R -extensions pop up; see Example 3.3. But, it will be used for further insights summarized in Corollary 4.6.(2), Proposition 4.14 and Corollary 4.15 below.

Theorem 3.21. Let (\mathbb{A}, σ) be a difference ring being reduced and connected with $\text{sconst} \mathbb{A} \setminus \{0\} = \mathbb{A}^*$. Let $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ be Π -extension of (\mathbb{A}, σ) with $\sigma(t) = \alpha t$ for some $\alpha \in \mathbb{A}^*$. Then $\text{sconst} \mathbb{A}[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst} \mathbb{A} \text{ and } m \in \mathbb{Z}\}$.

Proof. Take $\tilde{G} = (\mathbb{A}^*)_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$. Then $\tilde{G} = \mathbb{A}[t, \frac{1}{t}]^*$ by Lemma 3.2. Thus $\text{sconst } \mathbb{A}[t, \frac{1}{t}] = \text{sconst}_{\mathbb{A}[t, 1/t]^*} \mathbb{A}[t, \frac{1}{t}] = \text{sconst}_{\tilde{G}} \mathbb{A}[t, \frac{1}{t}] \stackrel{\text{Thm. 3.20}}{=} \{h t^m \mid h \in \text{sconst } \mathbb{A} \text{ and } m \in \mathbb{Z}\}$. \square

3.3. R -extensions

We start with the proof of the characterization theorem of R -extensions.

Proof 3.22. (Theorem 2.12.(3)). “ \Leftarrow ”: Let $m \in \{1, \dots, \lambda - 1\}$ and $g \in \mathbb{A} \setminus \{0\}$ with $\sigma(g) = \alpha^m g$. Since $\sigma(t^m) = \alpha^m t^m$, it follows that $\sigma(g t^{\lambda-m}) = g t^{\lambda-m}$, i.e., $g t^{\lambda-m} \in \text{const } \mathbb{A}[t]$. Clearly $g t^{\lambda-m} \notin \mathbb{A}$ which implies that $g t^{\lambda-m} \notin \text{const } \mathbb{A}$.
“ \Rightarrow ”: Let $g = \sum_{i=0}^{\lambda-1} g_i t^i \in \mathbb{A}[t] \setminus \mathbb{A}$ with $\sigma(g) = g$. Thus $g_r \neq 0$ for some $r \in \{1, \dots, \lambda - 1\}$. By coefficient comparison we get $\sigma(g_r) = \alpha^{\lambda-r} g_r$ with $\lambda - r \in \{1, \dots, \lambda - 1\}$. Let t be an R -monomial and let $m := \text{ord}(\alpha) < \lambda$. Then with $g = 1 \in \mathbb{A} \setminus \{0\}$ we have that $\sigma(g) = 1 = \alpha^m 1 = \alpha^m g$. A contradiction to the first statement. \square

Finally, we work out properties for the set of semi-constants. Since the proof of the following theorem is completely analogous to the proof of Proposition 3.19, it is skipped.

Proposition 3.23. Let (\mathbb{A}, σ) be a difference ring with $G \leq \mathbb{A}^*$ and $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[x], \sigma)$ be an R -extension of (\mathbb{A}, σ) with $\alpha = \frac{\sigma(x)}{x} \in G$ and $\lambda := \text{ord}(x) = \text{ord}(\alpha) > 1$. Then $\text{sconst}_G \mathbb{A}[x] = \{h x^m \mid h \in \text{sconst}_G \mathbb{A}, 0 \leq m < \lambda\}$ and $\text{sconst}_G \mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}[x]^*$.

As in Theorem 3.20 we will lift this result from the group $G \leq \mathbb{A}^*$ to

$$\tilde{G} = G_{\mathbb{A}}^{\mathbb{A}[x]} = \{h x^m \mid h \in G \text{ and } m \in \{0, \dots, \lambda - 1\}\} \leq \mathbb{A}[x]^*.$$

We remark that there is the following subtlety. We have to assume that $\mathbb{A}[x]$ is reduced in order to prove the result below. In order to take care of this extra property, further investigations will be necessary in Subsection 4.1.

Theorem 3.24. Let $(\mathbb{A}[x], \sigma)$ be an R -extension of (\mathbb{A}, σ) and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. If $\mathbb{A}[x]$ is reduced, then $\text{sconst}_{\tilde{G}} \mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}[x]^*$ for $\tilde{G} = G_{\mathbb{A}}^{\mathbb{A}[x]}$.

Proof. Let $\alpha := \frac{\sigma(x)}{x} \in \mathbb{A}^*$ and $n = \text{ord}(\alpha) = \text{ord}(x)$. Let $g \in \text{sconst}_{\tilde{G}} \mathbb{A}[x] \setminus \{0\}$, i.e., $\sigma(g) = u x^m g$ with $u \in G$ and $0 \leq m < n$. Since $x^{m n} = 1$, $\sigma(g^n) = u^n g^n$ with $u^n \in G$. First suppose that $v := g^n \in \mathbb{A}$. Since $\mathbb{A}[x]$ is reduced, $v \neq 0$ and thus $v \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$, i.e., $g(g^{n-1}/v) = 1$. Hence g is invertible, i.e., $g \in \mathbb{A}[x]^*$.

Otherwise, suppose that $v := g^n \notin \mathbb{A}$. Define $a := u^n \in G$. We consider two sub-cases. Suppose that there are a $k > 0$ and a $w \in \mathbb{A} \setminus \{0\}$ with $\sigma(w) = a^k w$. Then $w \in \text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Hence $\sigma((g^n)^k/w) = (g^n)^k/w$, i.e., $c := (g^n)^k/w \in \mathbb{K}$, and since $\mathbb{A}[x]$ is reduced, $c \neq 0$. Thus (as above) $g(g^{k n-1}/w/c) = 1$ and therefore $g \in \mathbb{K}[x]^*$.

Finally, suppose that there are no $k > 0$ and $w \in \mathbb{A} \setminus \{0\}$ with $\sigma(w) = a^k w$. Hence by Theorem 3.17 there is the Π -extension $(\mathbb{A}[t, \frac{1}{t}], \sigma)$ of (\mathbb{A}, σ) with $\sigma(t) = a t$ ($a \in G \leq \mathbb{A}^*$). Let $v = g^n = \sum_{i=0}^{n-1} v_i x^i \in \mathbb{A}[x] \setminus \mathbb{A}$. Then $\sigma(v) = a v$ and thus by coefficient comparison it follows that $\sigma(v_i) = a \alpha^{n-i} v_i$ for some $v_i \in \mathbb{A} \setminus \{0\}$ with $1 \leq i < n$. Hence $\sigma(\frac{v_i}{t}) = \alpha^{n-i} \frac{v_i}{t}$, and thus $\sigma(\frac{v_i^n}{t^n}) = \frac{v_i^n}{t^n}$. Since \mathbb{A} is reduced, we have $v_i^n \neq 0$, and consequently $\frac{v_i^n}{t^n} \in \text{const } \mathbb{A}[t, \frac{1}{t}] \setminus \mathbb{A}$, a contradiction that t is a Π -monomial. Thus this case can be excluded. Summarizing, any element in $\text{sconst}_{\tilde{G}} \mathbb{A}[x] \setminus \{0\}$ is from $\mathbb{A}[x]^*$. \square

4. Nested $R\Pi\Sigma^*$ -extensions and simple $R\Pi\Sigma^*$ -extensions

We explore the set of semi-constants. First we deal with nested R -extensions in Subsection 4.1 and with nested $\Pi\Sigma^*$ -extensions in Subsection 4.2. Finally, we obtain Theorems 2.22 and 2.24 for nested $R\Pi\Sigma^*$ -extensions in Subsection 4.3. In addition, we work out further structural properties of (simple) $R\Pi\Sigma^*$ -extensions.

4.1. Nested R -extensions

We derive a first result of the semi-constants by applying iteratively Proposition 3.23.

Proposition 4.1. Let (\mathbb{A}, σ) be a difference ring with $G \leq \mathbb{A}^*$ and $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle$ be an R -extension of (\mathbb{A}, σ) with $\frac{\sigma(x_i)}{x_i} \in G$ and $n_i = \text{ord}(x_i)$. Then $\text{sconst}_G \mathbb{E} = \{h x_1^{m_1} \dots x_e^{m_e} \mid h \in \text{sconst}_G \mathbb{A} \text{ and } 0 \leq m_i < n_i \text{ for } 1 \leq i \leq e\}$ and $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$.

In order to treat nested R -extensions, we proceed as follows. Let $(\mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle, \sigma)$ be an R -extension of (\mathbb{A}, σ) with $\lambda_i = \text{ord}(x_i)$ and $\sigma(x_i) = \alpha_i x_i$. Moreover, take the polynomial ring $R = \mathbb{A}[y_1, \dots, y_e]$ and define $\alpha'_i = \alpha_i|_{x_1 \rightarrow y_1, \dots, x_{i-1} \rightarrow y_{i-1}}$. Then we obtain the automorphism $\sigma' : R \rightarrow R$ by $\sigma'|_{\mathbb{A}} = \sigma$ and $\sigma(y_i) = \alpha_i y_i$, i.e., (R, σ') is a difference ring extension of (\mathbb{A}, σ) . Thus by iterative application of the construction used for Lemma 2.6 it follows that $\mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle$ is isomorphic to R/I where I is the ideal

$$I = \langle y_1^{\lambda_1} - 1, \dots, y_e^{\lambda_e} - 1 \rangle \quad (21)$$

in R . In particular, we obtain the automorphism $\sigma'' : R/I \rightarrow R/I$ defined by $\sigma''(f + I) = \sigma'(f) + I$ and it follows that the difference ring $(\mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle, \sigma)$ is isomorphic to $(R/I, \sigma'')$; here $f \in \mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle$ is mapped to $f' + I$ with $f' = f|_{x_1 \rightarrow y_1, \dots, x_e \rightarrow y_e}$.

Take $G = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}} \leq \mathbb{E}^*$. In order to show that $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ holds as claimed in Corollary 4.3 below, we use Gröbner bases theory.

Lemma 4.2. Let $\lambda_i \in \mathbb{N} \setminus \{0\}$. Then the zero-dimensional ideal I given in (21) in the polynomial ring $R = \mathbb{F}[y_1, \dots, y_e]$ is radical.

Proof. The ideal I is zero-dimensional. Since \mathbb{F} has characteristic 0, it is perfect. We therefore apply Seidenberg's criterion (algorithm) given in [10, Thm. 8.22]. Define $f_i = y_i^{\lambda_i} - 1$. Then for each i ($1 \leq i \leq e$) we have that $f_i \in R \cap \mathbb{F}[y_i]$ and $\gcd(f_i, \frac{d}{dy_i} f_i) = \gcd(y_i^{\lambda_i} - 1, \lambda_i y_i^{\lambda_i-1}) = 1$. Thus [10, Thm. 8.22] implies that $\langle f_1, \dots, f_e \rangle$ is radical. \square

Corollary 4.3. Let (\mathbb{E}, σ) be an R -extension of a difference field (\mathbb{F}, σ) and let $G = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Then \mathbb{E} is reduced and $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$.

Proof. The difference ring (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ is isomorphic to $(R/I, \sigma'')$ as defined above with (21) where $\mathbb{A} = \mathbb{F}$. Suppose that \mathbb{E} is not reduced. Then there are an $f \in \mathbb{E} \setminus \{0\}$ and an $n > 0$ with $f^n = 0$. Hence there is an $h \in R$ with $h + I \neq I$ and $(h + I)^n = h^n + I = I$. This implies that $h \notin I$ and $h^n \in I$. Therefore I is not radical, a contradiction to Lemma 4.2. Hence \mathbb{E} is reduced. Thus we can apply Theorem 3.24 iteratively and it follows that $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$. \square

4.2. Nested $\Pi\Sigma^*$ -extensions

In Corollary 4.6 we will characterize the set of semi-constants within $\Pi\Sigma^*$ -extensions. Part 1 will deal with the general case. Part 2 assumes in addition that the ground ring is reduced and connected. In this setting, we rely on the following two lemmas.

Lemma 4.4. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a $\Pi\Sigma^*$ -extension of (\mathbb{A}, σ) . If \mathbb{A} is reduced, $\mathbb{A}\langle t \rangle$ is reduced. If \mathbb{A} is reduced and connected, $\mathbb{A}\langle t \rangle$ is reduced and connected.

Proof. Let t be a Π -monomial. Moreover, let \mathbb{A} be reduced. Now take $f = \sum_i f_i t^i \in \mathbb{A}\langle t \rangle = \mathbb{A}[t, \frac{1}{t}]$ with $f \neq 0$ and $f^n = 0$ for some $n > 0$. Since \mathbb{A} is reduced, $f \notin \mathbb{A}$. Let $m \in \mathbb{Z}$ be maximal such that $f_m \neq 0$. Then the coefficient of t^{nm} in f^n is f_m^n . Hence $f_m^n = 0$ and thus f_m is a nilpotent element in \mathbb{A} , a contradiction.

Now let \mathbb{A} be reduced and connected and take $f = \sum_i f_i t^i \in \mathbb{A}\langle t \rangle = \mathbb{A}[t, \frac{1}{t}]$ with $f^2 = f$ and $f \notin \{0, 1\}$. Since \mathbb{A} is connected, $f \notin \mathbb{A}$. Let m be maximal such that $f_m \neq 0$. If $m > 0$, then the coefficient of t^{2m} in f^2 is f_m^2 and thus with $f^2 = f$ we have that $f_m^2 = 0$; a contradiction that \mathbb{A} is reduced. Otherwise, if $m = 0$, we take \bar{m} minimal with $f_{\bar{m}} \neq 0$. Note that $\bar{m} < 0$ since $f \notin \mathbb{A}$. As above, it follows that $f_{\bar{m}}^2 = 0$, again a contradiction. Summarizing, if \mathbb{A} is reduced (and connected), $\mathbb{A}[t, \frac{1}{t}]$ is reduced (and connected). For a Σ^* -monomial t , the same implications hold since $\mathbb{A}\langle t \rangle = \mathbb{A}[t] \leq \mathbb{A}[t, \frac{1}{t}]$. \square

If \mathbb{A} is reduced, the shift behaviour of Π -monomials does not depend on Σ^* -monomials.

Lemma 4.5. Let (\mathbb{E}, σ) be a $\Pi\Sigma^*$ -ring extension of (\mathbb{A}, σ) where \mathbb{A} is reduced. Then the generators can be reordered such that we get the form $\mathbb{E} = \mathbb{A}\langle t_1 \rangle \dots \langle t_p \rangle \langle s_1 \rangle \dots \langle s_e \rangle$ where the t_i are Π -monomials and the s_i are Σ^* -monomials.

Proof. Let $\mathbb{E} = \mathbb{A}\langle t_1 \rangle \dots \langle t_e \rangle$. By iterative application of Lemma 4.4 it follows that \mathbb{E} is reduced. Let t_i be a Π -monomial where $\alpha = \sigma(t_i)/t_i \in \mathbb{A}\langle t_1 \rangle \dots \langle t_{i-1} \rangle$ depends on a Σ^* -monomial t_j with $j < i$. Then we can reorder the generators such that we get $\mathbb{H} = \mathbb{A}\langle t_1 \rangle \dots \langle t_{j-1} \rangle \langle t_{j+1} \rangle \dots \langle t_{i-1} \rangle$; here we forget σ and argue purely in the given ring. In particular, $\alpha \in \mathbb{H}\langle t_j \rangle = \mathbb{H}[t_j] \setminus \mathbb{H}$. Since α is invertible, $\alpha \in \mathbb{H}$ by Lemma 3.2; a contradiction. Summarizing, for all Π -monomials t_j we have that $\sigma(t_j)/t_j$ is free of Σ^* -monomials. Thus we can shuffle all Π -monomials to the left and all Σ^* -monomials to the right and obtain again a $\Pi\Sigma^*$ -extension. \square

Corollary 4.6. Let (\mathbb{E}, σ) be a $\Pi\Sigma^*$ -extension of (\mathbb{A}, σ) with $\mathbb{E} = \mathbb{A}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_e \rangle$.

(1) Let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ and let $\tilde{G} = G_{\mathbb{A}}^{\mathbb{E}}$. If (\mathbb{E}, σ) is a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{A}, σ) , then $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ where

$$\text{sconst}_{\tilde{G}} \mathbb{E} = \{h t_1^{m_1} \dots t_e^{m_e} \mid h \in \text{sconst}_G \mathbb{A} \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial}\}.$$

(2) If \mathbb{A} is reduced and connected and $\text{sconst} \mathbb{A} \setminus \{0\} = \mathbb{A}^*$, then

$$\text{sconst} \mathbb{E} \setminus \{0\} = \{h t_1^{m_1} \dots t_e^{m_e} \mid h \in \mathbb{A}^* \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial}\} = \mathbb{E}^*. \quad (22)$$

(3) If \mathbb{A} is a field then we have that (22).

Proof. The first part is proven by induction on the number e of extensions. If $e = 0$, nothing has to be shown. Now suppose that the first part holds and consider one extra \tilde{G} -simple $\Pi\Sigma^*$ -monomial t_{e+1} on top. Define $\tilde{G} = \tilde{G}_{\mathbb{E}}^{\mathbb{E}\langle t_{e+1} \rangle} = G_{\mathbb{A}}^{\mathbb{E}\langle t_{e+1} \rangle}$. If t_i is a

Σ^* -monomial, $\tilde{G} = \tilde{G}$. Together with Theorem 3.12 it follows that $\text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}] = \text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}] = \text{sconst}_{\tilde{G}}\mathbb{E}$ and $\text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}] \setminus \{0\} \leq \mathbb{E}^* \leq \mathbb{E}[t_{e+1}]^*$. If t_i is a Π -monomial, we have $\sigma(t_{e+1})/t_{e+1} \in \tilde{G}$. Hence Theorem 3.20 yields $\text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}, \frac{1}{t_{e+1}}] = \{h t_{e+1}^m \mid m \in \mathbb{Z} \text{ and } h \in \text{sconst}_{\tilde{G}}\mathbb{E}\}$ and thus by the induction assumption we have that

$$\text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}, \frac{1}{t_{e+1}}] = \{h t_1^{m_1} \dots t_{e+1}^{m_{e+1}} \mid h \in \text{sconst}_G\mathbb{A} \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial}\}$$

and thus $\text{sconst}_{\tilde{G}}\mathbb{E}[t_{e+1}, \frac{1}{t_{e+1}}] \setminus \{0\} \leq \mathbb{E}[t_{e+1}, \frac{1}{t_{e+1}}]^*$. This completes the induction step. Similarly, the first equality of part 2 follows by Theorems 3.14 and 3.21. The second equality follows by Lemmas 3.2 and 4.4. Since any field is connected and reduced and $\text{sconst}\mathbb{A} \setminus \{0\} = \mathbb{A}^*$ by Lemma 3.13, part 3 follows by part 2. \square

Restricting to Σ^* -extensions, the above result simplifies as follows.

Corollary 4.7. Let (\mathbb{E}, σ) be a Σ^* -extension of (\mathbb{A}, σ) . Then the following holds.

- (1) If $G \leq \mathbb{A}^*$ with $\text{sconst}_G\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$, then $\text{sconst}_G\mathbb{E} = \text{sconst}_G\mathbb{A}$.
- (2) If \mathbb{A} is reduced and $\text{sconst}\mathbb{A} \setminus \{0\} = \mathbb{A}^*$, then \mathbb{E} is reduced and $\text{sconst}\mathbb{E} = \text{sconst}\mathbb{A}$.
- (3) If \mathbb{A} is a field, then $\text{sconst}\mathbb{E} \setminus \{0\} = \mathbb{A}^* = \mathbb{A} \setminus \{0\}$.

4.3. $R\Pi\Sigma^*$ -extensions and their simple and single-rooted restrictions

We turn to the set of semi-constants within nested $R\Pi\Sigma^*$ -extensions. The case of simple and single-rooted $R\Pi\Sigma^*$ -extensions is immediate.

Proof 4.8. (Theorem 2.22). This follows by Corollary 4.6.(1) and Proposition 4.1. \square

Likewise, simple $R\Pi\Sigma^*$ -extension can be treated if they are built in a particular form.

Theorem 4.9. Let (\mathbb{H}, σ) be an R -extension of a difference field (\mathbb{F}, σ) and let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{H}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_e \rangle$ be a simple $\Pi\Sigma^*$ -extension of (\mathbb{H}, σ) . Let $G = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{H}}$ and define $\tilde{G} = G_{\mathbb{H}}^{\mathbb{E}}$. Then we have $\text{sconst}_{\tilde{G}}\mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ where

$$\text{sconst}_{\tilde{G}}\mathbb{E} = \{h t_1^{m_1} \dots t_e^{m_e} \mid h \in \text{sconst}_G\mathbb{H}, m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial}\}.$$

Proof. By Cor. 4.3, $\text{sconst}_G\mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$. Hence the result follows by Cor. 4.6.(1). \square

Next, we show that simple $R\Pi\Sigma^*$ -extensions can be always brought to the shape as assumed in Theorem 4.9. This will finally produce a proof of Theorem 2.24.

Lemma 4.10. Let (\mathbb{A}, σ) be a difference ring with a group $G \leq \mathbb{A}^*$ and let (\mathbb{E}, σ) be a G -simple $R\Pi\Sigma^*$ -extension of (\mathbb{A}, σ) .

- (1) The $R\Pi\Sigma^*$ -monomials can be reordered to the form $\mathbb{E} = \mathbb{A}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_e \rangle$ with $r, p \in \mathbb{N}$ ($0 \leq r \leq p \leq e$) such that the following holds.
 - For all i ($1 \leq i \leq r$), t_i is an R -monomial with $\sigma(t_i)/t_i = u_i t_1^{z_1} \dots t_{i-1}^{z_{i-1}}$ for some root of unity $u_i \in G$ and $z_i \in \mathbb{N}$.
 - For all i ($r < i \leq p$), t_i is a Π -monomial with $\sigma(t_i)/t_i = u_i t_1^{z_1} \dots t_{i-1}^{z_{i-1}}$ for some $u_i \in G$ and $z_i \in \mathbb{Z}$.
 - For all i ($p < i \leq e$), t_i is a Σ^* -monomial with $\sigma(t_i) - t_i \in \mathbb{A}\langle t_1 \rangle \langle t_2 \rangle \dots \langle t_{i-1} \rangle$.
- (2) For any $f \in G_{\mathbb{A}}^{\mathbb{E}}$ which depends on a Π -monomial we have that $\text{ord}(f) = 0$.

Proof. We show the lemma by induction on the number of $R\Pi\Sigma^*$ -monomials. Suppose that the lemma holds for e extensions. Now let $\mathbb{E} = \mathbb{A}\langle t_1 \rangle \dots \langle t_e \rangle$ and consider the $R\Pi\Sigma^*$ -monomial t_{e+1} on top of \mathbb{E} . By the induction assumption we can reorder \mathbb{E} such that it has the desired form (all R -monomials are on the left, all Π -monomials are in the middle and all Σ^* -monomials are on the right). If t_{e+1} is a Σ^* -monomial, the required shape is fulfilled. If t_{e+1} is an R -monomial, observe that $\alpha := \sigma(t_{e+1})/t_{e+1} \in G_{\mathbb{A}}^{\mathbb{E}}$. Since $\text{ord}(\alpha) = \text{ord}(t_{e+1}) > 1$ by Theorem 2.12.(3), α is free of Π -monomials by the induction assumption and (by definition) free of Σ^* -monomials. Thus we can shuffle t_{e+1} to the left (such that all $\Pi\Sigma^*$ -monomials are to the right), and the required shape is satisfied. Similarly, if t_{e+1} is a Π -monomial, $\sigma(t_{e+1})/t_{e+1} \in G_{\mathbb{A}}^{\mathbb{E}}$ is free of Σ^* -monomials by definition and we can shuffle t_{e+1} to the left such that all Σ^* -monomials are to the right. This completes the first part of the lemma. Now let $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_{e+1} \rangle$ be in the desired ordered form. If x_{e+1} is a Σ^* -monomial, we have that $G_{\mathbb{A}}^{\mathbb{E}\langle x_{e+1} \rangle} = G_{\mathbb{A}}^{\mathbb{E}}$. Thus the second part holds by the induction assumption. If x_{e+1} is an R -extension, also all x_i with $1 \leq i \leq e$ are R -monomials, and the second statement holds trivially. Finally, let x_{e+1} be a Π -monomial and take $f \in G_{\mathbb{A}}^{\mathbb{E}\langle x_{e+1} \rangle}$. If $f \in \mathbb{E}$ and f depends on Π -monomials, we have again that $\text{ord}(f) = 0$ by the induction assumption. To this end, suppose that f depends on x_{e+1} and we have that $\text{ord}(f) = n > 0$. Then $f = u x_{e+1}^m$ where $m \neq 0$ and $u \in \mathbb{E}^*$. Since $f^n = 1$, $u^n x_{e+1}^{mn} = 1$ where $u^n \neq 0$. Hence x_{e+1} is not transcendental over \mathbb{E} , a contradiction to the definition of a Π -monomial. Thus $\text{ord}(f) = n = 0$. This completes the proof. \square

Proof 4.11. (Theorem 2.24). By Lemma 4.10 we can reorder the simple $R\Pi\Sigma^*$ -extension such that Theorem 4.9 is applicable. \square

In the remaining part of this section we deliver insight into the structure of (simple) $R\Pi\Sigma^*$ -extensions. First observe that a tower of simple $R\Pi\Sigma^*$ -extensions is again simple.

Lemma 4.12. Let (\mathbb{A}, σ) be a difference ring with a group $G \leq \mathbb{A}^*$ and let $(\mathbb{A}, \sigma) \leq (\mathbb{H}, \sigma) \leq (\mathbb{E}, \sigma)$ be $R\Pi\Sigma^*$ -extensions. Then $(G_{\mathbb{A}}^{\mathbb{H}})_{\mathbb{H}}^{\mathbb{E}} = G_{\mathbb{A}}^{\mathbb{E}}$. Moreover, if $(\mathbb{A}, \sigma) \leq (\mathbb{H}, \sigma)$ is G -simple and $(\mathbb{H}, \sigma) \leq (\mathbb{E}, \sigma)$ is $G_{\mathbb{A}}^{\mathbb{H}}$ -simple, then $(\mathbb{A}, \sigma) \leq (\mathbb{E}, \sigma)$ is G -simple.

Further, the reordering as described in Lemma 4.10 is also possible if one relaxes the condition that the $R\Pi\Sigma^*$ -extension is simple but requires that the ground ring is a field.

Lemma 4.13. Let (\mathbb{E}, σ) be a $R\Pi\Sigma^*$ -ring extension of a difference field (\mathbb{F}, σ) . Then (\mathbb{E}, σ) can be reordered to the form $\mathbb{E} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \langle t_1 \rangle \dots \langle t_p \rangle \langle s_1 \rangle \dots \langle s_e \rangle$ where the x_i are R -monomials, the t_i are Π -monomials and the s_i are Σ^* -monomials.

Proof. First we try to shuffle all R -extensions to the front. Suppose that this fails at the first time. Then there are an R -extension (\mathbb{H}, σ) of (\mathbb{F}, σ) , a $\Pi\Sigma^*$ -extension (\mathbb{G}, σ) of (\mathbb{H}, σ) with $\mathbb{G} = \mathbb{H}\langle y_1 \rangle \dots \langle y_l \rangle$ and an R -extension $(\mathbb{G}\langle x \rangle, \sigma)$ of (\mathbb{G}, σ) with $\alpha = \sigma(x)/x$ in which y_l occurs. Note that \mathbb{H} is reduced by Corollary 4.3, and \mathbb{G} is reduced by iterative application of Lemma 4.4. Write $\alpha = \sum_i f_i y_l^i$. Let $m \neq 0$ such that $f_m \neq 0$ and such that $|m| \geq 1$ is maximal (we remark that $m < 0$ can only happen if y_l is a Π -monomial). By the choice of m , we have that the coefficient of y_l^{mn} in α^n is f_m^n . Hence with $\alpha^n = 1$ it follows that $f_m^n = 0$, a contradiction to the assumption that \mathbb{G} is reduced. Therefore we can shuffle all R -monomials to the left and all $\Pi\Sigma^*$ -monomials to the right. Since the nested R -extension is reduced by Corollary 4.3, we can apply Lemma 4.5 to reorder the $\Pi\Sigma^*$ -monomials further as claimed in the statement. \square

By definition any (nested) Σ^* -extension is also a simple Σ^* -extension. If the ground ring is reduced and connected, we obtain the following stronger result.

Proposition 4.14. Let (\mathbb{G}, σ) be a difference ring where \mathbb{G} is reduced and connected and where $\text{sconst} \mathbb{G} \setminus \{0\} = \mathbb{G}^*$. Then a $\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of (\mathbb{G}, σ) is simple.

Proof. Let $\mathbb{E} = \mathbb{G}\langle t_1 \rangle \dots \langle t_e \rangle$. By Lemma 4.5 we may suppose that the generators are ordered such that the $t_1 \dots, t_p$ are Π -monomials and the $t_{p+1} \dots, t_e$ are Σ^* -monomials. By Corollary 4.6.(2) we have that $\frac{\sigma(t_i)}{t_i} \in \mathbb{G}\langle t_1 \rangle \dots \langle t_{i-1} \rangle^* = (\mathbb{G}^*)_{\mathbb{G}}^{\mathbb{G}\langle t_1 \rangle \dots \langle t_{i-1} \rangle}$ with $1 \leq i \leq p$. Thus the Π -monomials t_i are \mathbb{G}^* -simple. Moreover, the Σ^* -monomials t_i on top are all \mathbb{G}^* -simple by definition. Summarizing $(\mathbb{F}, \sigma) \leq (\mathbb{E}, \sigma)$ is simple. \square

In other words, for a reduced and connected difference ring (\mathbb{A}, σ) (e.g., if \mathbb{A} is a field) the notions of $\Pi\Sigma^*$ -ring extension and simple $\Pi\Sigma^*$ -ring extension are equivalent. The situation becomes rather different if the ring is, e.g., not connected; see Example 2.20. But, for single-rooted $R\Pi\Sigma^*$ -extensions over a difference field, the situation is again tame.

Corollary 4.15. A single-rooted $R\Pi\Sigma^*$ -extension (\mathbb{E}, σ) of a field (\mathbb{G}, σ) is simple.

Proof. By definition the $R\Pi\Sigma^*$ -extension can be reordered to the form (2.21). Since \mathbb{G} is a field, $\text{sconst} \mathbb{G} \setminus \{0\} = \mathbb{G}^*$. By Proposition 4.14 the Π -extension $(\mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle, \sigma)$ of (\mathbb{G}, σ) is simple. Since $\frac{\sigma(x_i)}{x_i} \in \mathbb{G}^*$ for $1 \leq i \leq u$, the R -monomials x_i are \mathbb{G}^* -simple. Since also the Σ^* -monomials s_i are \mathbb{G}^* -simple, we conclude that $(\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)$ is simple. \square

5. The algorithmic machinery I: order, period, factorial order

An important ingredient for the development of our summation algorithms is the knowledge of the order (see its definition in (10) and the corresponding Problem O), the period and the factorial order. In (\mathbb{A}, σ) we define the period of $h \in \mathbb{A}^*$ by

$$\text{per}(h) = \begin{cases} 0 & \text{if } \nexists n > 0 \text{ s.t. } \sigma^n(h) = h \\ \min\{n > 0 \mid \sigma^n(h) = h\} & \text{otherwise;} \end{cases}$$

and the factorial order of h by

$$\text{ford}(h) = \begin{cases} 0 & \text{if } \nexists n > 0 \text{ s.t. } h_{(n)} = 1 \\ \min\{n > 0 \mid h_{(n)} = 1\} & \text{otherwise.} \end{cases}$$

Using the properties of the automorphism σ and Lemma 3.4 it is easy to see that the \mathbb{Z} -modules generated by $\text{ord}(h)$, $\text{per}(h)$ and $\text{ford}(h)$ are $\langle \text{ord}(h) \rangle = \text{ord}(h)\mathbb{Z} = \{k \in \mathbb{Z} \mid h^k = 1\}$, $\langle \text{per}(h) \rangle = \text{per}(h)\mathbb{Z} = \{k \in \mathbb{Z} \mid \sigma^k(h) = h\}$, and $\langle \text{ford}(h) \rangle = \text{ford}(h)\mathbb{Z} = \{k \in \mathbb{Z} \mid h_{(k)} = 1\}$, respectively. In addition, the following basic properties hold.

Lemma 5.1. Let (\mathbb{A}, σ) be a difference ring with $\alpha, h \in \mathbb{A}^*$. Then the following holds.

- (1) If $\alpha \in (\text{const} \mathbb{A})^*$, then $\text{per}(\alpha) = 1$ and $\text{ford}(\alpha) = \text{ord}(\alpha)$.
- (2) If $\sigma(h) = \alpha h$, then $\text{per}(h) = \text{ford}(\alpha)$.
- (3) If $\text{ord}(\alpha) > 0$ and $\text{per}(\alpha) > 0$, then $\text{per}(\alpha) \mid \text{ford}(\alpha) \mid \text{per}(\alpha) \text{ord}(\alpha)$ and

$$\text{ford}(\alpha) = \min\{i \mid \text{per}(\alpha) \mid 1 \leq i \leq \text{ord}(\alpha) \text{ and } \alpha_{(i \text{ per}(\alpha))} = 1\} > 0. \quad (23)$$

Proof. (1) Since $\sigma(\alpha) = \alpha$, $\text{per}(\alpha) = 1$. Since $\alpha_{(n)} = \alpha^n$ for $n \geq 0$, $\text{ford}(\alpha) = \text{ord}(\alpha)$.
(2) By Lemma 3.4.(4) we have that $\sigma^n(h) = h$ iff $\alpha_{(n)} = 1$. Hence $\text{per}(h) = \text{ford}(\alpha)$.
(3) Take $p = \text{per}(\alpha) > 0$ and $v = \text{ord}(\alpha) > 0$. Then we have that

$$\alpha_{(p^v)} = \alpha \sigma(\alpha) \dots \sigma^{p^v-1}(\alpha) = (\alpha \sigma(\alpha) \dots \sigma^{p-1}(\alpha))^v = \alpha^v \sigma(\alpha^v) \dots \sigma^{p-1}(\alpha^v) = 1.$$

Consequently, we can choose $n = \text{ord}(\alpha) \text{per}(\alpha)$ to obtain $\alpha_{(n)} = 1$. In particular, for any $i \geq 0$ with $\alpha_{(i)} = 1$ we have that $1 = \frac{\sigma(1)}{1} = \frac{\sigma(\alpha_{(i)})}{\alpha_{(i)}} = \frac{\sigma^i(\alpha)}{\alpha}$. Hence $\text{per}(\alpha) | i$. Thus the smallest λ with $\alpha_{(\lambda)} = 1$ is given by (23). In particular, $\text{per}(\alpha) | \text{ford}(\alpha) | \text{ord}(\alpha) \text{per}(\alpha)$. \square

We will present methods to calculate the order, period and factorial order for the elements of $(\mathbb{A}^*)_{\mathbb{A}}^{\mathbb{E}}$ of a simple R -extension $(\mathbb{E}, \sigma) \geq (\mathbb{G}, \sigma)$ by recursion. First, we assume that the orders of the R -monomials in $(\mathbb{E}, \sigma) \geq (\mathbb{G}, \sigma)$ are already computed and show how the orders of the elements of $(\mathbb{A}^*)_{\mathbb{A}}^{\mathbb{E}}$ can be determined.

Lemma 5.2. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle$ be an R -extension of (\mathbb{A}, σ) and define

$$\alpha := u x_1^{z_1} \dots x_e^{z_e} \in (\mathbb{A}^*)_{\mathbb{A}}^{\mathbb{E}} \quad (24)$$

with $u \in \mathbb{A}^*$ and $z_i \in \mathbb{N}$. Then $\text{ord}(\alpha) > 0$ iff $\text{ord}(u) > 0$. If $\text{ord}(u) > 0$, then

$$\text{ord}(\alpha) = \text{lcm}(\text{ord}(u), \frac{\text{ord}(x_1)}{\text{gcd}(\text{ord}(x_1), z_1)}, \dots, \frac{\text{ord}(x_e)}{\text{gcd}(\text{ord}(x_e), z_e)}). \quad (25)$$

Proof. If $e = 0$, the lemma holds. Now let $n := \text{ord}(\alpha) > 0$. Suppose that $1 \neq (x_1^{z_1} \dots x_e^{z_e})^n = x_1^{nz_1} \dots x_e^{nz_e}$. Let i be maximal such that $\text{ord}(x_i) \nmid z_i n$. Then there is an s with $0 < s < \text{ord}(x_i)$ with $x_i^{\text{ord}(x_i)-s} = u^n x_1^{z_1} \dots x_{i-1}^{z_{i-1}} \in \mathbb{A}\langle x_1 \rangle \dots \langle x_{i-1} \rangle$ which contradicts to the construction that $x_i^{\text{ord}(x_i)} = 1$ is the defining relation of the R -monomial. Thus $(x_1^{z_1} \dots x_e^{z_e})^n = 1$ and $u^n = 1$, i.e., $\text{ord}(u) > 0$ and $\text{ord}(x_1^{z_1} \dots x_e^{z_e}) > 0$. In particular, $\text{ord}(\alpha) = \text{lcm}(\text{ord}(u), \text{ord}(x_1^{z_1} \dots x_e^{z_e}))$. By similar arguments we can show that $(x_1^{z_1})^n = \dots = (x_e^{z_e})^n = 1$ and consequently $\text{ord}(x_1^{z_1} \dots x_e^{z_e}) = \text{lcm}(\text{ord}(x_1^{z_1}), \dots, \text{ord}(x_e^{z_e}))$. Since also $\text{ord}(x_i^{z_i}) = \frac{\text{ord}(x_i)}{\text{gcd}(\text{ord}(x_i), z_i)}$ holds, the identity (25) is proven.

Conversely, suppose that $\text{ord}(u) > 0$. Then the value of the right right hand side of (25) is positive. Denote it by n . Then one can check that $\alpha^n = 1$. Therefore $\text{ord}(\alpha) > 0$. \square

In the next lemma we set the stage to calculate the period and factorial order.

Lemma 5.3. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle$ be an R -extension of (\mathbb{A}, σ) where we have $\text{per}(x_i) > 0$ for $1 \leq i \leq e$. Let $\alpha \in (\mathbb{A}^*)_{\mathbb{A}}^{\mathbb{E}}$ as in (24) with $z_1, \dots, z_e \in \mathbb{N}$ and $u \in \mathbb{A}^*$.

(1) Then $\text{per}(\alpha) > 0$ iff $\text{per}(u) > 0$. If $\text{per}(u) > 0$, then

$$\text{per}(\alpha) = \min(1 \leq j \leq \mu | \sigma^j(\alpha) = \alpha \text{ and } j | \mu) \quad (26)$$

with $\mu = \text{lcm}(\text{per}(u), \text{per}(x_{i_1}), \dots, \text{per}(x_{i_k}))$ where $\{i_1, \dots, i_k\} = \{i : \text{ord}(x_i) \nmid z_i\}$.

(2) We have that $\text{ford}(\alpha) > 0$ iff $\text{ford}(u) > 0$.

(3) If $\text{per}(u), \text{ord}(u) > 0$, then $\text{ford}(\alpha) > 0$ and $0 < \text{per}(\alpha) | \text{ford}(\alpha) | \text{per}(\alpha) \text{ord}(\alpha)$.

(4) If the values $\text{ord}(x_i)$ and $\text{per}(x_i)$ for $1 \leq i \leq e$ and the values $\text{per}(u) > 0$ and $\text{ord}(u) > 0$ are given explicitly, then $\text{per}(\alpha)$ and $\text{ford}(\alpha)$ can be calculated.

Proof. (1) Suppose that $\text{per}(u) > 0$. Then $\mu > 0$. In particular, it follows that $\sigma^\mu(\alpha) = \alpha$. Consequently, $\text{per}(\alpha) > 0$ with $\text{per}(\alpha) | \mu$. Hence we have (26). Conversely, suppose that $\text{per}(\alpha) > 0$. Then with $\nu := \text{lcm}(\text{per}(\alpha), \text{per}(x_1), \dots, \text{per}(x_e)) > 0$ we get $u x_1^{z_1} \dots x_e^{z_e} =$

$\alpha = \sigma^\nu(\alpha) = \sigma^\nu(u) x_1^{z_1} \dots x_e^{z_e}$. Thus $\sigma^\nu(u) = u$, and consequently $\text{ord}(u) > 0$.

(2) Since $\text{ord}(x_i)$ and $\text{per}(x_i) > 0$, it follows that $\text{ford}(x_i) > 0$ by Lemma 5.1.(3) for all $1 \leq i \leq e$. If $\text{ford}(u) > 0$, take $\nu = \text{lcm}(\text{ford}(u), \text{ford}(x_1), \dots, \text{ford}(x_e)) > 0$. By Lemma 3.4.(1), $\alpha_{(\nu)} = 1$ and hence $\text{ford}(\alpha) > 0$. Conversely, if $\text{ford}(\alpha) > 0$, take $\nu' = \text{lcm}(\text{ford}(\alpha), \text{ford}(x_1), \dots, \text{ford}(x_e)) > 0$. Then again by Lemma 3.4.(1): $1 = \alpha_{(\nu')} = (u x_1^{z_1} \dots x_e^{z_e})_{(\nu')} = u_{(\nu')}$. Thus $\text{ford}(u) > 0$.

(3) By part 1, $\text{per}(\alpha) > 0$. And with $\text{ord}(u) > 0$ and Lemma 5.2 it follows that $\text{ord}(\alpha) > 0$. By Lemma 5.1.(3), $\text{per}(\alpha) | \text{ford}(\alpha) | \text{ord}(\alpha) \text{per}(\alpha)$. In particular, $\text{ford}(\alpha) > 0$.

(4) If $\text{per}(u)$ and the values $\text{per}(x_i)$ are given, μ from part 1 can be computed. In particular, if $\text{ord}(u)$ and $\text{ord}(x_i)$ are given explicitly, $\text{ord}(\alpha)$ can be calculated by Lemma 5.2. Thus $\text{per}(\alpha)$ can be determined by (26) and then $\text{ford}(\alpha)$ can be computed by (23). \square

Example 5.4. (1) Take $\alpha = u = -1 \in \mathbb{Q}$. We get $\text{ord}(\alpha) = 2$. In addition, $\text{per}(-1) = 1$. Moreover, $1 = \text{per}(-1) | \text{ford}(-1) | \text{per}(-1) \text{ord}(-1) = 2$. Hence (26) yields $\text{ford}(-1) = 2$.

(2) Consider the R -extension $(\mathbb{Q}[x], \sigma)$ of (\mathbb{Q}, σ) with $\sigma(x) = -x$ and $\text{ord}(x) = 2$, and take $\alpha = -x$. We get $\text{ord}(\alpha) = \text{lcm}(\text{ord}(-1), \text{ord}(x)) = 2$ by (25). With $\mu = \text{lcm}(\text{per}(-1), \text{per}(x)) = 2$ we get $\text{per}(\alpha) = 2$ by using (26). Furthermore, we get $2 = \text{per}(\alpha) | \text{ford}(\alpha) | \text{per}(\alpha) \text{ord}(\alpha) = 4$. Hence with (26) we get $\text{ford}(\alpha) = 4$.

(3) Consider the R -extension $(\mathbb{K}(k)[x], \sigma)$ of $(\mathbb{K}(k), \sigma)$ with $\sigma(x) = \iota x$ and $\text{ord}(x) = 4$ from Example 2.14. We have $\text{per}(x) = 4$. Take $\alpha = x$. We obtain the following bounds $4 = \text{per}(\alpha) | \text{ford}(\alpha) | \text{per}(\alpha) \text{ord}(\alpha) = 16$. Thus with (26) we determine $\text{ford}(\alpha) = 8$.

Combining the two lemmas from above we arrive at the following result.

Proposition 5.5. Let $(\mathbb{A}\langle x_1 \rangle \dots \langle x_e \rangle, \sigma)$ be a simple R -extension of (\mathbb{A}, σ) such that for $1 \leq i \leq e$ we have that $\sigma(x_i)/x_i = u_i x_1^{m_{i,1}} \dots x_{i-1}^{m_{i,i-1}}$ with $u_i \in \mathbb{A}^*$ and $m_{i,j} \in \mathbb{N}$. Then the following holds.

- (1) $\text{ord}(u_i) > 0$ for $1 \leq i \leq e$. In particular, if the values $\text{ord}(u_i)$ are given explicitly (are computable), then the values $\text{ord}(x_i)$ are computable.
- (2) If $\text{per}(u_i) > 0$ for $1 \leq i \leq e$, then $\text{per}(x_i) > 0$ for $1 \leq i \leq e$. In particular, if the values of $\text{ord}(u_i)$ and $\text{per}(u_i)$ for $1 \leq i \leq e$ are given explicitly (are computed), the values $\text{per}(x_i)$ for all $1 \leq i \leq e$ are computable.

Proof. (1) By iterative application of Lemma 5.3 it follows that $\text{ord}(u_i) > 0$ for all $1 \leq i \leq e$. Moreover, suppose that $\text{ord}(u_i)$ is given for $1 \leq i \leq e$. Furthermore, assume that the values $\text{ord}(x_i)$ for $1 \leq i \leq s$ with $s < e$ are already determined. Then define $\alpha = \sigma(x_s)/x_s$. By (25) we obtain $\text{ord}(\alpha)$ and thus $\text{ord}(x_s) = \text{ord}(\alpha)$ by Theorem 2.12.(3). This completes the induction step.

(2) Suppose that $\text{per}(u_i) > 0$ for $1 \leq i \leq e$. In addition, suppose that we have shown already that $d_i = \text{per}(x_i) > 0$ for $1 \leq i < s$ with $s \leq e$. Define $\alpha = \sigma(x_s)/x_s$. By Lemma 5.3 we have $\text{per}(\alpha) > 0$ and $\text{ford}(\alpha) > 0$. By Lemma 5.1.(2) it follows that $\text{per}(x_s) = \text{ford}(\alpha) > 0$. If the values $\text{ord}(u_i)$ are given explicitly, we can compute $\text{ord}(\alpha)$ by part 1. If $\text{per}(u_s)$ is given explicitly and d_1, \dots, d_{s-1} are given (are already computed), $\text{per}(\alpha)$ can be computed with Lemma 5.1.(3). Hence $\text{ford}(\alpha)$ can be calculated with (23). Thus we get $\text{ord}(x_s) = \text{ford}(\alpha)$ by Lemma 5.1.(2) which completes the induction step. \square

If we restrict to the case that the ground domain is a field \mathbb{F} and all roots of unity of \mathbb{F} are constants, we end up at the following properties of R -extensions.

Corollary 5.6. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}\langle x_1 \rangle \dots \langle x_e \rangle$ be a simple R -extension of a difference field (\mathbb{F}, σ) with constant field \mathbb{K} such that all roots of unity in \mathbb{F} are constants (e.g., if (\mathbb{F}, σ) is strong constant-stable). Then the following holds.

(1) For $1 \leq i \leq e$ we have that

$$\sigma(x_i)/x_i = u_i x_1^{m_{i,1}} \dots x_{i-1}^{m_{i,i-1}} \quad (27)$$

for some root of unity $u_i \in \mathbb{K}^*$ with $\text{ord}(u_i) \mid \text{ord}(x_i)$ and $m_{i,j} \in \mathbb{N}$.

(2) $(\mathbb{K}\langle x_1 \rangle \dots \langle x_e \rangle, \sigma)$ is a simple R -extension of (\mathbb{K}, σ) .

(3) Let $\alpha = u x_1^{z_1} \dots x_e^{z_e} \in (\mathbb{K}^*)_{\mathbb{K}}^{\mathbb{K}\langle x_1 \rangle \dots \langle x_e \rangle}$ with $z_1, \dots, z_e \in \mathbb{N}$ and $u \in \mathbb{K}^*$. Then

$$\text{ord}(u) > 0 \Leftrightarrow \text{ord}(\alpha) > 0 \Leftrightarrow \text{per}(\alpha) > 0 \Leftrightarrow \text{ford}(\alpha) > 0.$$

(4) If (\mathbb{K}, σ) is computable and Problem O is solvable in \mathbb{K}^* then the values of $\text{ord}(\alpha)$, $\text{per}(\alpha)$ and $\text{ford}(\alpha)$ are computable for all $\alpha \in (\mathbb{K}^*)_{\mathbb{K}}^{\mathbb{K}\langle x_1 \rangle \dots \langle x_e \rangle}$.

(5) Problem O is solvable in $(\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ if it is solvable in \mathbb{K}^* and (\mathbb{F}, σ) is computable.

Proof. (1) By definition we have that (27) with $m_i \in \mathbb{N}$ and $u_i \in \mathbb{F}^*$. By Lemma 5.2 it follows that $\text{ord}(u_i) > 0$ and $\text{ord}(u_i) \mid \text{ord}(x_i)$. In particular, $u_i \in \mathbb{K}^*$ since all roots of unity from \mathbb{F} are constants by assumption.

(2) It is immediate that (\mathbb{H}, σ) with $\mathbb{H} = \mathbb{K}\langle x_1 \rangle \dots \langle x_e \rangle$ forms a difference ring. Since $\text{const } \mathbb{E} = \text{const } \mathbb{F} = \mathbb{K}$, (\mathbb{H}, σ) is a simple R -extension of (\mathbb{K}, σ) .

(3) By part 1 we get $u_i \in \mathbb{K}^*$ and $\text{ord}(u_i) > 0$ for $1 \leq i \leq e$. In particular, $\text{per}(u_i) = 1$. With Proposition 5.5 we get $\text{per}(x_i) > 0$, and by Lemma 5.1.(1) we obtain $\text{per}(u) = 1$ and $\text{ford}(u) = \text{ord}(u)$. Thus the equivalences follow by Lemmas 5.2 and 5.3 (parts 1,2).

(4) Since $u_i \in \mathbb{K}^*$, the values of $\text{ord}(u_i) > 0$ can be determined by solving Problem O in \mathbb{K}^* . Thus by Proposition 5.5 the orders and periods of the x_i can be computed. Let $\alpha := u x_1^{z_1} \dots x_e^{z_e}$ with $u \in \mathbb{K}^*$ and $z_i \in \mathbb{N}$. Then by Lemma 5.2 and the computation of $\text{ord}(u)$ the order of α can be computed. Moreover, since $\text{per}(u) = 1$ and $\text{ord}(u) = \text{ford}(u)$ are given, we can invoke Lemma 5.3 to calculate the period and factorial order of α .

(5) Let α be given as in (24) with $u \in \mathbb{F}^*$ and $m_i \in \mathbb{N}$. By Lemma 5.2 $\text{ord}(\alpha) > 0$ iff $\text{ord}(u) > 0$. By assumption, $\text{ord}(u) > 0$ implies $u \in \mathbb{K}^*$. Thus, if $u \notin \mathbb{K}$, $\text{ord}(\alpha) = 0$. Otherwise, if $u \in \mathbb{K}^*$, we can apply part 4. \square

Finally, we are in the position to prove Theorem 2.26.(1).

Proof 5.7. (Theorem 2.26.(1)). Let (\mathbb{E}, σ) be a simple $R\Pi\Sigma^*$ -extension of (\mathbb{F}, σ) where (\mathbb{F}, σ) is computable and where any root of unity of \mathbb{F} is from $\mathbb{K} = \text{const } \mathbb{F}$. Reorder it to the shape as given in Lemma 4.10. In particular, the R -extension $(\mathbb{F}\langle t_1 \rangle \dots \langle t_r \rangle, \sigma)$ of (\mathbb{F}, σ) has the shape as given in Corollary 5.6.(1). Let $f \in (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Suppose first that f depends on a Π -monomial t_i . Now assume that $\text{ord}(f) = n > 0$, and let i be maximal such that a Π -monomial depends on f . Then $f = v t_i^m$ with $v \in \mathbb{F}\langle t_1 \rangle \dots \langle t_{i-1} \rangle^*$ and $m \in \mathbb{Z} \setminus \{0\}$. Hence $1 = f^n = v^n t_i^{m n}$ and thus t_i is not algebraically independent over $\mathbb{F}\langle t_1 \rangle \dots \langle t_{i-1} \rangle$; a contradiction. Consequently, if f depends on Π -monomials, $\text{ord}(f) = 0$. Otherwise, $f = u t_1^{m_1} \dots t_r^{m_r}$ with $u \in \mathbb{F}^*$ and $m_i \in \mathbb{N}$ where the t_i are all R -monomials. Therefore the value $\text{ord}(f)$ can be computed by Corollary 5.6.(5). \square

6. The algorithmic machinery II: Problem PMT

We aim at proving Theorems 2.23.(1) and 2.26.(2), i.e., providing recursive algorithms that reduce Problem PMT from a given $R\Pi\Sigma^*$ -extension to its ground ring (resp. field). For this reduction we assume that for the given ground ring (\mathbb{G}, σ) and given group $G \leq \mathbb{G}^*$ we have that $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$. This property guarantees that for any $\mathbf{f} \in G^n$ a \mathbb{Z} -basis of $M(\mathbf{f}, \mathbb{G})$ with rank $\leq n$ exists; see Lemma 2.16. In particular, we rely on the fact that there are algorithms available that solve Problem PMT in (\mathbb{G}, σ) for G . For concrete classes of difference fields (\mathbb{G}, σ) with these algorithmic properties we refer to Subsection 2.3.3.

6.1. A reduction strategy for $\Pi\Sigma^*$ -extensions

First, we treat the reduction for $\Pi\Sigma^*$ -extensions. More precisely, we will obtain

Theorem 6.1. Let (\mathbb{G}, σ) be a computable difference ring with $G \leq \mathbb{G}^*$ where $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$. Let (\mathbb{E}, σ) be a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) . Then $\text{sconst}_{G_{\mathbb{E}}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ and Problem PMT is solvable in (\mathbb{E}, σ) for $G_{\mathbb{E}}$ if it is solvable in (\mathbb{G}, σ) for G .

For the underlying reduction method we use the following two lemmas.

Lemma 6.2. Let $(\mathbb{A}[t], \sigma)$ be a Σ^* -extension of (\mathbb{A}, σ) and let $H \leq \mathbb{A}^*$ be a group with $\text{sconst}_H \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Then for $\mathbf{f} \in H^n$ we have that $M(\mathbf{f}, \mathbb{A}[t]) = M(\mathbf{f}, \mathbb{A})$.

Proof. “ \subseteq ”: Let $\mathbf{m} = (m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{A}[t])$ with $\mathbf{f} = (f_1, \dots, f_n) \in H^n$. Thus take $g \in \mathbb{A}[t] \setminus \{0\}$ with $\sigma(g) = f_1^{m_1} \dots f_n^{m_n} g$. Since $g \in \text{sconst}_H \mathbb{A}[t] \setminus \{0\}$, we have $g \in \text{sconst}_H \mathbb{A}$ by Theorem 3.12. Hence $\mathbf{m} \in M(\mathbf{f}, \mathbb{A})$. The inclusion \supseteq is obvious. \square

Lemma 6.3. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a Π -extension of (\mathbb{A}, σ) and let $H \leq \mathbb{A}^*$ with $\text{sconst}_H \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ and $\alpha := \sigma(t)/t \in H$. Let $\mathbf{f} = (f_1, \dots, f_n) \in (H_{\mathbb{A}}^{\mathbb{A}\langle t \rangle})^n$ with

$$f_i = h_i t^{e_i}, \quad h_i \in H, \quad e_i \in \mathbb{Z}.$$

Then $M(\mathbf{f}, \mathbb{A}\langle t \rangle) = M_1 \cap M_2$ where

$$\begin{aligned} M_1 &= \{(m_1, \dots, m_n) \mid (m_1, \dots, m_n, m_{n+1}) \in M((h_1, \dots, h_n, \frac{1}{\alpha}), \mathbb{A})\}, \\ M_2 &= \text{Ann}_{\mathbb{Z}}((e_1, \dots, e_n)) = \{(m_1, \dots, m_n) \in \mathbb{Z}^n \mid m_1 e_1 + \dots + m_n e_n = 0\}. \end{aligned}$$

Proof. “ \subseteq ”: Let $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{A}\langle t \rangle)$. Hence we can take $g \in \mathbb{A}\langle t \rangle \setminus \{0\}$ with $\sigma(g) = f_1^{m_1} \dots f_n^{m_n} g$, i.e., $g \in \text{sconst}_{\tilde{H}} \mathbb{A}\langle t \rangle \setminus \{0\}$ with $\tilde{H} = H_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$. Thus by Theorem 3.20 it follows that $g = \tilde{g} t^m$ with $m \in \mathbb{Z}$ and $\tilde{g} \in \text{sconst}_{\tilde{H}} \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Hence

$$\sigma(\tilde{g}) = f_1^{m_1} \dots f_n^{m_n} \alpha^{-m} \tilde{g} = h_1^{m_1} \dots h_n^{m_n} \alpha^{-m} \tilde{g} t^{m_1 e_1 + \dots + m_n e_n}.$$

Since $\tilde{g} \neq 0$, we conclude that $\sigma(\tilde{g}) \neq 0$. By coefficient comparison it follows then that $m_1 e_1 + \dots + m_n e_n = 0$, i.e., $(m_1, \dots, m_n) \in M_2$. Thus $\sigma(\tilde{g}) = h_1^{m_1} \dots h_n^{m_n} \alpha^{-m} \tilde{g}$ and consequently $(m_1, \dots, m_n, m) \in M((h_1, \dots, h_n, \frac{1}{\alpha}), \mathbb{A})$, i.e., $(m_1, \dots, m_n) \in M_1$.

“ \supseteq ”: Let $(m_1, \dots, m_n) \in M_1 \cap M_2$. Thus we can take $\tilde{g} \in \mathbb{A} \setminus \{0\}$ and $m \in \mathbb{Z}$ with $\sigma(\tilde{g}) = h_1^{m_1} \dots h_n^{m_n} \alpha^{-m} \tilde{g}$. Moreover, we have that $e_1 m_1 + \dots + e_n m_n = 0$. Thus $\sigma(\tilde{g} t^m) = (h_1 t^{e_1})^{m_1} \dots (h_n t^{e_n})^{m_n} \tilde{g}$ and therefore $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{A}\langle t \rangle)$. \square

Now we can deal with the underlying algorithm resp. proof of Theorem 6.1.

Proof 6.4. (Theorem 6.1). Let (\mathbb{G}, σ) be a difference ring and let $G \leq \mathbb{G}^*$ such that $\text{sconst}_G \mathbb{G} \setminus \{0\} \leq \mathbb{G}^*$ holds. Suppose that Problem PMT is solvable in (\mathbb{G}, σ) for G . Now let (\mathbb{E}, σ) be a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) as in the theorem with $\tilde{G} = G_{\mathbb{G}}^{\mathbb{E}}$ and let $\mathbf{f} \in \tilde{G}^n$. By Corollary 4.6.(1) it follows that $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ and together with Lemma 2.16 it follows that $M(\mathbf{f}, \mathbb{E}) = M(\mathbf{f}, \text{sconst}_{\tilde{G}} \mathbb{E})$ is a \mathbb{Z} -module. The calculation of a basis of $M(\mathbf{f}, \mathbb{E})$ will be accomplished by recursion/induction. If $\mathbb{E} = \mathbb{A}$, nothing has to be shown. Otherwise, let (\mathbb{A}, σ) be a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{G}, σ) in which we know how one can solve Problem PMT for $H = G_{\mathbb{G}}^{\mathbb{A}}$, and let $\mathbb{E} = \mathbb{A}\langle t \rangle$ where t is a H -simple $\Pi\Sigma^*$ -monomial. We have to treat two cases. First, suppose that t is a Σ^* -monomial. Then it follows that $\tilde{G} = G_{\mathbb{G}}^{\mathbb{E}} = G_{\mathbb{G}}^{\mathbb{A}} = H \leq \mathbb{A}^*$ and thus $\mathbf{f} \in H^n$. Hence we can activate Lemma 6.2 and it follows that $M(\mathbf{f}, \mathbb{E}) = M(\mathbf{f}, \mathbb{A})$. Thus by assumption we can compute a basis. Second, suppose that t is a H -simple Π -monomial. Then we can utilize Lemma 6.3: We calculate a basis of M_2 by linear algebra. Furthermore, we compute a basis of $M((h_1, \dots, h_n, \frac{1}{\alpha}), \mathbb{A})$ by the induction assumption (by recursion). Hence we can derive a basis of M_2 and thus of $M_1 \cap M_2 = M(\mathbf{f}, \mathbb{A}\langle t \rangle)$. This completes the proof. \square

Note that the reduction presented in Lemma 6.3 is accomplished by increasing the rank of M_1 by one. In general, the more Π -monomials are involved, the higher the rank will be in the arising Problems PMT of the recursions.

Looking closer at the reduction algorithm, we can extract the following shortcut, resp. a refined version of Theorem 2.12.(2).

Corollary 6.5. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let (\mathbb{H}, σ) be a G -simple Π -extension of (\mathbb{A}, σ) and let (\mathbb{E}, σ) be a Σ^* -extension of (\mathbb{H}, σ) . Then $G_{\mathbb{A}}^{\mathbb{E}} = G_{\mathbb{A}}^{\mathbb{H}}$ and the following holds.

- (1) $M(\mathbf{f}, \mathbb{E}) = M(\mathbf{f}, \mathbb{H})$ for any $\mathbf{f} \in (G_{\mathbb{A}}^{\mathbb{E}})^n$.
- (2) Let $\alpha \in G_{\mathbb{A}}^{\mathbb{E}}$. Then there is a Π -extension $(\mathbb{E}\langle t \rangle, \sigma)$ of (\mathbb{E}, σ) with $\sigma(t) = \alpha t$ iff there is a Π -extension $(\mathbb{H}\langle t \rangle, \sigma)$ of (\mathbb{H}, σ) with $\sigma(t) = \alpha t$.

Proof. Note that $G_{\mathbb{A}}^{\mathbb{E}} \leq \mathbb{H}^*$. Hence by iterative application of Lemma 6.2 part 1 is proven. Part 2 follows by part 1 and Theorem 2.12.(2). \square

If one restricts to the special case that (\mathbb{G}, σ) is a $\Pi\Sigma^*$ -field with $G = \mathbb{G}^*$, the presented reduction techniques boil down to the reduction presented in [24, Theorem 8]. The major contribution here is that Theorem 6.1 can be applied for any computable difference ring (\mathbb{G}, σ) with the properties given in Theorem 6.1. Subsequently, we utilize this additional flexibility to tackle (nested) R -extensions.

6.2. A reduction strategy for R -extensions and thus for $R\Pi\Sigma^*$ -extensions

First, we treat the special case of single-rooted and simple R -extensions.

Lemma 6.6. Let (\mathbb{A}, σ) be a difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[x], \sigma)$ be an R -extension of (\mathbb{A}, σ) with $\sigma(x) = \alpha x$ where $\alpha \in G$; let $\mathbf{f} = (f_1, \dots, f_n) \in G^n$. Then $M(\mathbf{f}, \mathbb{A}[x]) = \{(m_1, \dots, m_n) \mid (m_1, \dots, m_{n+1}) \in M((f_1, \dots, f_n, \frac{1}{\alpha}), \mathbb{A})\}$.

Proof. Let $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{A}[x])$. Hence there is a $g \in \text{sconst}_G \mathbb{A}[x] \setminus \{0\}$ with $\sigma(g) = f_1^{m_1} \dots f_n^{m_n} g$. By Proposition 3.23 it follows that $g = \tilde{g} x^m$ with $\tilde{g} \in \mathbb{A} \setminus \{0\}$ and $m \in \mathbb{N}$. Thus

$$\sigma(\tilde{g}) = f_1^{m_1} \dots f_n^{m_n} \alpha^{-m} \tilde{g} \quad (28)$$

and hence $(m_1, \dots, m_n, m) \in M((f_1, \dots, f_n, \frac{1}{\alpha}), \mathbb{A})$. Conversely, if $(m_1, \dots, m_n, m) \in M((f_1, \dots, f_n, 1/\alpha), \mathbb{A})$, there is a $\tilde{g} \in \mathbb{A} \setminus \{0\}$ with (28). Therefore we conclude that $\sigma(\tilde{g} t^m) = f_1^{m_1} \dots f_n^{m_n} \tilde{g} t^m$ which implies that $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{A}[x])$. \square

As a consequence we obtain the proof of our Theorem 2.23.(1).

Proof 6.7. (Theorem 2.23.(1)). Since Problem PMT is solvable in (\mathbb{G}, σ) for G , it follows by Theorem 6.1 that Problem PMT is solvable in (\mathbb{H}, σ) for \tilde{G} with $\mathbb{H} = \mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle$ and that $\text{sconst}_{\tilde{G}} \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$. Thus by iterative applications of Lemma 6.6 and Proposition 3.23 we conclude that Problem PMT is solvable in (\mathbb{H}, σ) for \tilde{G} with $\mathbb{H} = \mathbb{H}\langle x_1 \rangle \dots \langle x_u \rangle$ and that $\text{sconst}_{\tilde{G}} \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$. Finally, by applying again Theorem 6.1 it follows that Problem PMT is solvable in (\mathbb{E}, σ) for \tilde{G} . \square

In order to tackle the more general case that the R -extensions are nested and that they might occur also in Π -extensions (see the underlying algorithms for Theorem 2.26.(2) in Proof 6.15 below), we require additional properties on the difference rings: they must be strong constant-stable; see Definition 2.25. With this extra condition the following structural property of the semi-constants holds. They factor into two parts: a factor which depends only on the R -monomials with constant coefficients and a factor which is free of the R -monomials.

Lemma 6.8. Let (\mathbb{A}, σ) be a difference ring which is constant-stable and let $G \leq \mathbb{A}^*$ be closed under σ where $\text{sconst}_G(\mathbb{A}, \sigma^k) \setminus \{0\} \leq \mathbb{A}^*$ for any $k > 0$. Let (\mathbb{E}, σ) be a simple R -extension of (\mathbb{A}, σ) with $\mathbb{E} = \mathbb{A}[x_1] \dots [x_e]$ where we have (27) with $m_{i,j} \in \mathbb{N}$ and $u_i \in G$ with $\text{per}(u_i) > 0$. Define

$$r := \begin{cases} \text{lcm}(\text{ford}(u_1), \dots, \text{ford}(u_e), \text{ford}(x_1), \dots, \text{ford}(x_e)) & \text{if } e > 0 \\ 1 & \text{if } e = 0. \end{cases} \quad (29)$$

Let $\tilde{G} = G_{\mathbb{A}}^{\mathbb{E}}$ with $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$. Then the following holds.

(1) $r > 0$. (2) For any $g \in \text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\}$ we have that

$$g = \tilde{g} h \quad (30)$$

with $\tilde{g} \in \text{sconst}_G(\mathbb{A}, \sigma^r) \setminus \{0\} \leq \mathbb{A}^*$ and $h \in \text{const}(\mathbb{K}[x_1, \dots, x_e], \sigma^r)^*$.

(3) If $\sigma(g) = v x_1^{m_1} \dots x_e^{m_e} g$ with $v \in G$, $m_i \in \mathbb{N}$, then $\sigma(\tilde{g}) = \lambda v \tilde{g}$ with $\lambda \in \mathbb{A}^*$, $\lambda^r = 1$.

Proof. Let $g \in \text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\}$, i.e., $\sigma(g) = v x_1^{m_1} \dots x_e^{m_e} g$ with $v \in G$ and $m_i \in \mathbb{Z}$. Let r be given as in (29). If $e = 0$, i.e., $r = 1$, the lemma holds by taking $\tilde{g} := g \in \mathbb{A}^*$ and $h = 1$. Otherwise, we may suppose that $e > 0$.

(1) Let $1 \leq i \leq e$. By Proposition 5.5.(1) it follows that $\text{ord}(u_i) > 0$. Together with the assumption that $\text{per}(u_i) > 0$ we have that $\text{ford}(u_i) > 0$ by Lemma 5.1.(3). Moreover, by Proposition 5.5.(2) it follows that $\text{per}(x_i) > 0$. Again with $\text{ord}(x_i) > 0$ and $\text{per}(x_i) > 0$ it follows that $\text{ford}(x_i) > 0$ by Lemma 5.1.(3). Therefore $r > 0$.

(2) By the choice of r it follows that for all $1 \leq i \leq e$ we have

$$(u_i)_{(r)} = 1, \quad (x_i)_{(r)} = 1 \text{ and } \sigma^r(x_i) = x_i; \quad (31)$$

the last equality follows by Lemma 5.3.(3). Moreover, by Lemma 3.4 we conclude that

$$\sigma^r(g) = (v x_1^{m_1} \dots x_e^{m_e})_{(r)} g = v_{(r)} (x_1)_{(r)}^{m_1} \dots (x_e)_{(r)}^{m_e} g = \tilde{u} g$$

with $\tilde{u} := v_{(r)}$. Since G is closed under σ , we have that $\tilde{u} \in G$. Write $g = \sum_{\mathbf{s} \in S} g_{\mathbf{s}} \mathbf{x}^{\mathbf{s}}$ where $S \subseteq \mathbb{N}^e$ is finite, $g_{\mathbf{s}} \in \mathbb{F}^*$ and for $(s_1, \dots, s_e) \in S$ and $\mathbf{x} = (x_1, \dots, x_e)$ we use the multi-index notation $\mathbf{x}^{\mathbf{s}} = x_1^{s_1} \dots x_e^{s_e}$. In particular, we suppose that if $\mathbf{s}, \mathbf{s}' \in S$ with $\mathbf{x}^{\mathbf{s}} = \mathbf{x}^{\mathbf{s}'}$ then $\mathbf{s} = \mathbf{s}'$. Then by coefficient comparison w.r.t. $\mathbf{x}^{\mathbf{i}}$ and using (31) we obtain $\sigma^r(g_{\mathbf{i}}) = \tilde{u} g_{\mathbf{i}}$ for any $\mathbf{i} \in S$. Note that $g_{\mathbf{i}} \in \text{sconst}_G(\mathbb{A}, \sigma^r) \setminus \{0\} \leq \mathbb{A}^*$. Hence for any $\mathbf{s}, \mathbf{r} \in S$ we have that $\sigma^r(g_{\mathbf{s}}/g_{\mathbf{r}}) = g_{\mathbf{s}}/g_{\mathbf{r}}$. Thus it follows that $g_{\mathbf{s}}/g_{\mathbf{r}} \in (\text{const}(\mathbb{A}, \sigma^r))^* = \mathbb{K}^*$, i.e., for all $s \in S$ we have that $g_{\mathbf{s}} = c_{\mathbf{s}} \tilde{g}$ for some $c_{\mathbf{s}} \in \mathbb{K}^*$ and $\tilde{g} \in \text{sconst}_G(\mathbb{A}, \sigma^r) \setminus \{0\} \leq \mathbb{A}^*$ with

$$\sigma^r(\tilde{g}) = \tilde{u} \tilde{g}. \quad (32)$$

Consequently, $g = \tilde{g} h$ with $h = \sum_{\mathbf{s} \in S} c_{\mathbf{s}} \mathbf{x}^{\mathbf{s}}$. Since $g \in \mathbb{A}^*$, $h \in \mathbb{K}[x_1, \dots, x_e]^*$. Finally, with (31) we conclude that $h \in \text{const}(\mathbb{K}[x_1, \dots, x_e], \sigma^r)^*$.

(3) Taking $\mathbf{s} = (s_1, \dots, s_e) \in S$, it is easy to see that there is exactly one $\mathbf{s}' \in S$ with

$$\sigma(c_{\mathbf{s}} \mathbf{x}^{\mathbf{s}} \tilde{g}) = v x_1^{m_1} \dots x_e^{m_e} c_{\mathbf{s}'} \mathbf{x}^{\mathbf{s}'}.$$

This means that on both sides the same monomial $\mathbf{x}^{\mathbf{s}' + (m_1, \dots, m_e)}$ in reduced form occurs. By coefficient comparison this gives $\sigma(\tilde{g}) = v u_1^{-s_1} \dots u_e^{-s_e} \frac{c_{\mathbf{s}'}}{c_{\mathbf{s}}} \tilde{g}$. Thus with (31) and Lemma 3.4 we get $\sigma^r(\tilde{g}) = v_{(r)} (\frac{c_{\mathbf{s}'}}{c_{\mathbf{s}}})^r \tilde{g} = \tilde{u} (\frac{c_{\mathbf{s}'}}{c_{\mathbf{s}}})^r \tilde{g}$. Hence with (32) we obtain $(\frac{c_{\mathbf{s}'}}{c_{\mathbf{s}}})^r = 1$. Finally, with $\lambda := u_1^{-s_1} \dots u_e^{-s_e} \frac{c_{\mathbf{s}'}}{c_{\mathbf{s}}}$ we have that $\sigma(\tilde{g}) = \lambda v \tilde{g}$ with $\lambda^r = 1$ and $\lambda \in \mathbb{A}^*$. \square

Specializing \mathbb{A} to a strong constant-stable difference field, the lemma reads as follows.

Corollary 6.9. Let (\mathbb{F}, σ) be a difference field with $\mathbb{K} = \text{const} \mathbb{F}$ which is strong constant-stable. Let (\mathbb{E}, σ) be a simple R -extension of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}[x_1] \dots [x_e]$ such that (27) holds with $m_{i,j} \in \mathbb{N}$, $u_i \in \mathbb{K}^*$, and define (29). Let $\tilde{G} = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Then: (1) $r > 0$. (2) For any $g \in \text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\}$ we have (30) with $\tilde{g} \in \mathbb{F}^*$ and $h \in \text{const}(\mathbb{K}[x_1, \dots, x_e], \sigma^r)^*$. (3) If $\sigma(g) = v x_1^{m_1} \dots x_e^{m_e} g$ with $v \in \mathbb{F}^*$, $m_i \in \mathbb{Z}$, then $\sigma(\tilde{g}) = \lambda v \tilde{g}$ with $\lambda \in \mathbb{K}^*$, $\lambda^r = 1$.

Proof. Since $u_i \in \mathbb{K}^*$ by Corollary 5.6.(1), $\text{per}(u_i) = 1$. Define $G = \mathbb{F}^*$ which is closed under σ . In particular, $\text{sconst}_G(\mathbb{F}, \sigma^k) \setminus \{0\} = \mathbb{F}^*$ for any $k > 0$. In addition, $\text{sconst}_{\tilde{G}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ by Corollary 4.3. Thus we can apply Lemma 6.8. The corollary follows by observing that $\lambda \in \mathbb{F}^*$ with $\lambda^r = 1$. Then by our assumption it follows that $\lambda \in \mathbb{K}^*$. \square

With this result we get the following reduction tactic for simple R -extensions.

Lemma 6.10. Let (\mathbb{F}, σ) be a difference field with $\mathbb{K} = \text{const} \mathbb{F}$ which is strong constant-stable. Let (\mathbb{E}, σ) be a simple R -extension of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}[x_1] \dots [x_e]$ where we have (27) with $m_{i,j} \in \mathbb{N}$ and $u_i \in \mathbb{K}^*$. Define $r > 0$ as given in (29) and choose⁸ a set $\{\alpha_1, \dots, \alpha_s\} \subseteq \mathbb{K}^*$ of r -th roots of unity which generate multiplicatively all r -th roots of unity of \mathbb{K} . Let $G = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ and let $\mathbf{f} = (f_1, \dots, f_n) \in G^n$ with $f_i = \tilde{f}_i h_i$ where $\tilde{f}_i \in \mathbb{F}^*$ and $h_i = x_1^{z_{i,1}} \dots x_e^{z_{i,e}}$ with $z_{i,j} \in \mathbb{N}$. Then

$$M(\mathbf{f}, \mathbb{E}) = \{(m_1, \dots, m_n) \mid (m_1, \dots, m_{n+s}) \in M_1 \cap M_2\} \quad (33)$$

⁸ In principal, we could also take one primitive r th root of unity α . However, if $\alpha \notin \mathbb{K}$, we have to extend the constant field. By efficiency reasons we prefer to stay in the original field. We remark that extending the constant field would not produce further relations.

where

$$\begin{aligned} M_1 &= M((\tilde{f}_1, \dots, \tilde{f}_n, \alpha_1, \dots, \alpha_s), \mathbb{F}), \\ M_2 &= M((h_1, \dots, h_n, \frac{1}{\alpha_1}, \dots, \frac{1}{\alpha_s}), \mathbb{K}[x_1] \dots [x_e]). \end{aligned}$$

Proof. Let $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{E})$, i.e., there is a $g \in \text{sconst}_G \mathbb{E} \setminus \{0\}$ with $\sigma(g) = f_1^{m_1} \dots f_n^{m_n} g$. Hence by Corollary 6.9 it follows that $g = \tilde{g} h$ with $\tilde{g} \in \mathbb{F}^*$ and $h \in \mathbb{K}[x_1] \dots [x_e]^*$. In particular, $\sigma(\tilde{g}) = \tilde{f}_1^{m_1} \dots \tilde{f}_n^{m_n} \lambda \tilde{g}$ for $\lambda \in \mathbb{K}^*$ being an r th root of unity. Hence we can take $m_{n+1}, \dots, m_{n+s} \in \mathbb{N}$ such that $\lambda = \alpha_1^{m_{n+1}} \dots \alpha_s^{m_{n+s}}$. Consequently,

$$\sigma(\tilde{g}) = \tilde{f}_1^{m_1} \dots \tilde{f}_n^{m_n} \alpha_1^{m_{n+1}} \dots \alpha_s^{m_{n+s}} \tilde{g}, \quad (34)$$

which yields

$$\sigma(h) = h_1^{m_1} \dots h_n^{m_n} \alpha_1^{-m_{n+1}} \dots \alpha_s^{-m_{n+s}} h. \quad (35)$$

Then (34) and (35) imply $(m_1, \dots, m_{n+s}) \in M_1 \cap M_2$. Conversely, let $(m_1, \dots, m_n) \in M_1 \cap M_2$. I.e., there are $m_i \in \mathbb{N}$, $\tilde{g} \in \mathbb{F}^*$ and $h \in \mathbb{K}[x_1] \dots [x_e]^*$ s.t. (34) and (35) hold. Therefore $\sigma(\tilde{g} h) = f_1^{m_1} \dots f_n^{m_n} \tilde{g} h$ which implies that $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{E})$. \square

The following remarks are in place. By Corollary 4.3 it follows that $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ and thus $M(\mathbf{f}, \mathbb{E})$ in Lemma 6.10 has a \mathbb{Z} -basis with rank $\leq n$. In particular, we can compute such a basis as follows. First note that both M_1 and M_2 given in Lemma 6.10 have \mathbb{Z} -bases with rank $\leq n + s$: for M_1 this follows since \mathbb{F} is a field. Moreover, if one takes $\mathbb{H} = \mathbb{K}[x_1] \dots [x_e] \leq \mathbb{E}$ and $H = (\mathbb{K}^*)_{\mathbb{K}}^{\mathbb{H}}$, it follows by Corollary 4.3 that $\text{sconst}_H \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$ and thus a \mathbb{Z} -basis exists with rank $\leq n + s$. Summarizing, we can determine a \mathbb{Z} -basis of $M(\mathbf{f}, \mathbb{E})$ by using (33) if bases of M_1 and M_2 are available.

Example 6.11. Take the $\Pi\Sigma^*$ -field $(\mathbb{K}(k), \sigma)$ over $\mathbb{K} = \mathbb{Q}(\iota)$ with $\sigma(k) = k + 1$ and consider the R -extension $(\mathbb{K}(k)[x], \sigma)$ of $(\mathbb{K}(k), \sigma)$ with $\sigma(x) = \iota x$ and $\text{ord}(x) = 4$ from Example 2.9. In order to obtain a degree bound in Example 7.6 below, we need a basis of $M = M(\mathbf{f}, \mathbb{K}(k)[x])$ with $\mathbf{f} = (kx, -\frac{x}{k+1})$. Here we will apply Lemma 6.10. By Example 5.4.(3) we get $\text{ford}(x) = 8$. With $u_1 = 1$ we determine $r = 8$ by (29). We define $\tilde{f}_1 = k$, $\tilde{f}_2 = -1/(k+1)$ and $h_1 = h_2 = x$. All 8th roots of unity of \mathbb{K} are generated by $\alpha_1 = \iota$. For the activation of the above lemma, we have to determine a basis of $M_1 = M((\tilde{f}_1, \tilde{f}_2, \alpha_1), \mathbb{K}(k)) = M((k, \frac{-1}{k+1}, \iota), \mathbb{K}(k))$. Here we use, e.g., the algorithms worked out in [24] (this is the base case of our machinery, see Subsection 2.3.3) and obtain the basis $\{(1, 1, 2), (0, 0, 4)\}$. Moreover, we compute the basis $\{(1, 1, 0), (0, 2, 0), (0, 0, 1)\}$ of $M_2 = M((h_1, h_2, \alpha_1), \mathbb{K}[x]) = M((x, x, \iota), \mathbb{K}[x])$, for details see Example 6.14 below. Thus a basis of $M_1 \cap M_2$ is $\{(1, 1, 2), (0, 0, 4)\}$ and we get the basis $\{(1, 1)\}$ of M .

By assumption (i.e., the base case in our recursion) a basis of M_1 can be determined. The calculation of a \mathbb{Z} -basis of M_2 can be accomplished by using the following proposition.

Proposition 6.12. Let (\mathbb{H}, σ) with $\mathbb{H} = \mathbb{K}[x_1] \dots [x_e]$ be a simple R -extension of (\mathbb{K}, σ) with a computable constant field \mathbb{K} and given $o_i = \text{ord}(x_i)$ for $1 \leq i \leq e$. Define $G = (\mathbb{K}^*)_{\mathbb{K}}^{\mathbb{H}}$ and let $\mathbf{f} = (f_1, \dots, f_n) \in G^n$ with given $\lambda_i := \text{ord}(f_i) > 0$ for $1 \leq i \leq n$. Then a basis of $M(\mathbf{f}, \mathbb{H})$ can be computed.

Proof. Define the finite sets

$$S := \{(n_1, \dots, n_e) \in \mathbb{N}^e \mid 0 \leq n_i < o_i\} \text{ and } \tilde{M} := \{(m_1, \dots, m_n) \in \mathbb{N}^n \mid 0 \leq m_i < \lambda_i\}.$$

Then loop through all vectors $\mathbf{m} = (m_1 \dots, m_n) \in \tilde{M}$ and check if there is a $g \in \mathbb{H}^*$ with $\sigma(g) = f_1^{m_1} \dots f_n^{m_n} g$. More precisely, we can make the Ansatz $g = \sum_{\mathbf{i} \in S} c_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ which leads to a linear system of equations in the $c_{\mathbf{i}}$ with coefficients from \mathbb{K} . Solving this system gives the solution space⁹ L and we can check if the considered \mathbf{m} from \tilde{M} is contained in $M(\mathbf{f}, \mathbb{H})$. In this way we can generate the subset $M' = \tilde{M} \cap M(\mathbf{f}, \mathbb{H})$. Denote by $\mathbf{b}_i \in \mathbb{K}^n$ the i th unit vector. We show that

$$\text{span}(M' \cup \{\lambda_1 \mathbf{b}_1, \dots, \lambda_n \mathbf{b}_n\}) = M(\mathbf{f}, \mathbb{H}). \quad (36)$$

Namely, since $M(\mathbf{f}, \mathbb{H})$ is a \mathbb{Z} -module (see the remarks above Example 6.11) and since $\lambda_i \mathbf{b}_i \in M(\mathbf{f}, \mathbb{H})$, the left hand side is contained in the right hand side. Conversely, suppose that $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{H})$. Then let $m'_i = m_i \bmod \lambda_i$, i.e., $0 \leq m'_i < \lambda_i$ with $m_i = m'_i + z_i \lambda_i$ for some $z_i \in \mathbb{Z}$. Thus $(m_1, \dots, m_n) = (m'_1, \dots, m'_n) + (\lambda_1 z_1, \dots, \lambda_n z_n)$ where $(m'_1, \dots, m'_n) \in \tilde{M}$ and $(\lambda_1 z_1, \dots, \lambda_n z_n) = z_1 (\lambda_1 \mathbf{b}_1) + \dots + z_n (\lambda_n \mathbf{b}_n)$. Consequently, (m_1, \dots, m_n) is an element of the left hand side of (36). Since the number of vectors of the span on the left hand side is finite, we can derive a \mathbb{Z} -basis of (36). \square

Remark 6.13. A basis of $M(\mathbf{f}, \mathbb{H})$ can be obtained more efficiently as follows. We start with the \mathbb{Z} -module which is given by the basis $B = \{\lambda_1 \mathbf{b}_1, \dots, \lambda_n \mathbf{b}_n\}$ where $\mathbf{b}_i \in \mathbb{K}^n$ is the i th unit vector. Now go through all elements from \tilde{M} . Take the first element \mathbf{m} from \tilde{M} . If it is in $\text{span}(B)$ (this can be easily checked), proceed to the next element. Otherwise, if it is an element from $M(\mathbf{f}, \mathbb{H})$ (for the check see the proof of Proposition 6.12), put it in B and transform the set again to a \mathbb{Z} -basis. More precisely, if we compose the rows \mathbf{b}_i to a matrix, it should yield a matrix in Hermite normal form. In this way, the membership tests for $\text{span}(B)$ can be carried out efficiently within the continuing calculation steps. We proceed until all elements of \tilde{M} are visited and update step by step B as described above. By construction we have that our $\text{span}(B)$ equals the left hand side of (36) and thus equals $M(\mathbf{f}, \mathbb{H})$. We remark that B consists always of n linearly independent vectors. However, the \mathbb{Z} -span is more and more refined.

Example 6.14 (Cont. Ex. 6.11). Take the R -extension $(\mathbb{K}[x], \sigma)$ of (\mathbb{K}, σ) with $\mathbb{K} = \mathbb{Q}(\iota)$, $\sigma(x) = \iota x$ and $\text{ord}(x) = 4$. We calculate a basis of $M(\mathbf{f}, \mathbb{K}[x])$ with $\mathbf{f} = (x, x, \iota)$ as presented in Remark 6.13. We start with $\{(4, 0, 0), (0, 4, 0), (0, 0, 4)\}$ whose rows form a matrix in Hermite normal form. Now we go through all elements of \tilde{M} , say in the order $\tilde{M} = \{(1, 0, 0), (2, 0, 0), (3, 0, 0), (0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 0, 1), (0, 0, 2), (0, 0, 3), (1, 1, 0), \dots\}$.

Since $(1, 0, 0) \notin \text{span}(B)$, we check if there is a $g \in \mathbb{K}[x] \setminus \{0\}$ with $\sigma(g) = x^1 x^0 \iota^0 g$; this is not the case. We continue with $(2, 0, 0)$. Here we have that $(2, 0, 0) \notin \text{span}(B)$. Now we check if there is a $g \in \mathbb{K}[x] \setminus \{0\}$ with $\sigma(g) = x^2 x^0 \iota^0 g$. Plugging in $g = g_0 + g_1 x + g_2 x^2 + g_3 x^3$ into $\sigma(g) = x^2 g$ gives the constraint $(g_0 - g_2)x^0 + \iota x(g_1 + \iota g_3) + x^2(-g_0 - g_2) + x^3(-g_1 - \iota g_3) = 0$ which leads to the solution $g = x + \iota x^3$. A basis of $\text{span}(B \cup \{(2, 0, 0)\})$ is $\{(2, 0, 0), (0, 4, 0), (0, 0, 4)\}$. Thus we update B to $B = \{(2, 0, 0), (0, 4, 0), (0, 0, 4)\}$. We have $(3, 0, 0) \notin \text{span}(B)$, but there is no $g \in \mathbb{K}[x] \setminus \{0\}$ with $\sigma(g) = x^3 g$. Similarly to $(1, 0, 0)$, also $(0, 1, 0)$ does not change B , and similarly to $(2, 0, 0)$, $(0, 2, 0)$ leads to the updated basis $B = \{(2, 0, 0), (0, 2, 0), (0, 0, 4)\}$. $(0, 3, 0)$ does not change B . However, for $(0, 0, 1) \notin \text{span}(B)$ we find $g = x$ with $\sigma(g) = x^0 x^0 \iota^1 g$ which yields $B = \{(2, 0, 0), (0, 2, 0), (0, 0, 1)\}$. We have that $(0, 0, 2), (0, 0, 3) \in \text{span}(B)$.

⁹ By arguments as in the proof of Lemma 2.16 it follows $\dim(L) \leq 1$.

Now we consider $(1, 1, 0) \notin \text{span}(B)$. We find $g = x + \iota x^3$ with $\sigma(g) = x^2 g$ (as already above). Hence we update B to $B = \{(1, 1, 0), (0, 2, 0), (0, 1, 0)\}$ (where the rows form a matrix in Hermite normal form). As it turns out, no further element from \tilde{M} changes B . Thus the found B is a basis of $M(\mathbf{f}, \mathbb{K}[x])$.

Proof 6.15. (Theorem 2.26.(2)). By Lemma 4.10 we can reorder the generators of the $R\Pi\Sigma^*$ -extension such that (\mathbb{E}, σ) is an \mathbb{F}^* -simple R -extension of (\mathbb{F}, σ) and (\mathbb{E}, σ) is a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{E}, σ) with $G = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Let $\mathbb{E} = \mathbb{F}[x_1] \dots [x_e]$ with u_i, α_i and $\mathbf{f} \in G^n$ with \tilde{f}_i and h_i as given in Lemma 6.10. By assumption we can compute a basis of M_1 as given in Lemma 6.10. Since Problem O is solvable in \mathbb{K}^* , we can compute $o_i = \text{ord}(x_i)$ and $\lambda_i = \text{ord}(u_i)$ by Corollary 5.6.(4). Thus we can use Proposition 6.12 to compute a basis of M_2 as posed in Lemma 6.10, and we get a basis of (33). Summarizing, we can solve Problem PMT in (\mathbb{E}, σ) for G . In particular, $\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ by Corollary 4.3. Hence by Theorem 6.1 we can solve Problem PMT for (\mathbb{E}, σ) in $G_{\mathbb{E}}^{\mathbb{E}}$. Since $G_{\mathbb{E}}^{\mathbb{E}} = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ by Lemma 4.12, the theorem is proven. \square

To this end, we work out the following shortcut, resp. refined version of Theorem 2.12.(3).

Corollary 6.16. Let (\mathbb{F}, σ) be a strong constant-stable difference field with constant field \mathbb{K} , and let $G \leq \mathbb{F}^*$ with $\text{sconst}_G \mathbb{F} \setminus \{0\} \leq \mathbb{F}^*$. Let (\mathbb{H}, σ) with $\mathbb{H} = \mathbb{F}[x_1] \dots [x_r]$ be a G -simple R -extension of (\mathbb{F}, σ) and let (\mathbb{E}, σ) be a $G_{\mathbb{F}}^{\mathbb{H}}$ -simple $\Pi\Sigma^*$ -extension of (\mathbb{H}, σ) .
(1) If $f \in G_{\mathbb{F}}^{\mathbb{H}}$ with $\text{ord}(f) > 0$, then $f \in (\mathbb{K}^* \cap G)_{\mathbb{F}}^{\mathbb{H}}$.
(2) $M(\mathbf{f}, \mathbb{E}) = M(\mathbf{f}, \mathbb{K}[x_1] \dots [x_r])$ for any $\mathbf{f} = (f_1, \dots, f_n) \in (G_{\mathbb{F}}^{\mathbb{H}})^n$ with $\text{ord}(f_i) > 0$.
(3) Let $\alpha \in G_{\mathbb{F}}^{\mathbb{H}}$ with $\text{ord}(\alpha) > 0$. Then there is an R -extension $(\mathbb{E}[t], \sigma)$ of (\mathbb{E}, σ) with $\frac{\sigma(t)}{t} = \alpha$ iff there is an R -extension $(\mathbb{K}[x_1] \dots [x_r][t], \sigma)$ of $(\mathbb{K}[x_1] \dots [x_r], \sigma)$ with $\frac{\sigma(t)}{t} = \alpha$.

Proof. (1) Let $f \in G_{\mathbb{F}}^{\mathbb{H}}$, i.e., $f = \alpha x_1^{m_1} \dots x_r^{m_r}$ where $\alpha \in G$ and $m_i \in \mathbb{N}$. With $\text{ord}(f) > 0$ and Corollary 5.6.(3) we have that $\text{ord}(\alpha) > 0$. Since (\mathbb{F}, σ) is strong constant-stable, $\alpha \in \mathbb{K}^*$. Thus $\alpha \in \mathbb{K}^* \cap G$ and hence $f \in (\mathbb{K}^* \cap G)_{\mathbb{F}}^{\mathbb{H}}$.
(2) Let $\mathbf{f} \in (G_{\mathbb{F}}^{\mathbb{H}})^n$ be given as above. By part 1, $f_i = \alpha_i x_1^{m_{i,1}} \dots x_r^{m_{i,r}}$ where the $\alpha_i \in \mathbb{K}$ are roots of unity and $m_{i,j} \in \mathbb{N}$. By Lemma 4.13 we may suppose that $\mathbb{E} = \mathbb{H}\langle t_1 \rangle \dots \langle t_k \rangle [s_1] \dots [s_e]$ where the t_i are Π -monomials and the s_i are Σ^* -monomials. By Corollary 6.5 we have that $M(\mathbf{f}, \mathbb{E}) = M(\mathbf{f}, \mathbb{H}\langle t_1 \rangle \dots \langle t_k \rangle)$. Now let $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{H}\langle t_1 \rangle \dots \langle t_k \rangle)$. Then there is a $g \in \mathbb{H}\langle t_1 \rangle \dots \langle t_k \rangle \setminus \{0\}$ with

$$\sigma(g) = u g \tag{37}$$

for some $u = a x_1^{\mu_1} \dots x_r^{\mu_r}$ with $\mu_i \in \mathbb{N}$ and with a being a root of unity from \mathbb{K} . By Corollary 5.6.(3) we get $\mu := \text{ord}(u) > 0$; in addition we have that $\mu' = \text{ford}(u) > 0$. By Theorem 4.9 it follows that $g = q t_1^{\nu_1} \dots t_k^{\nu_k}$ with $q \in \text{sconst}_G \mathbb{H} \setminus \{0\}$ and $\nu_i \in \mathbb{Z}$. Since $u^{\mu} = 1$, it follows with (37) that $\sigma(g^{\mu}) = g^{\mu}$. Now suppose that g depends on t_m with $1 \leq m \leq k$ being maximal. Then g^{μ} depends also on t_m which contradicts to $\text{const}_{\mathbb{H}} \langle t_1 \rangle \dots \langle t_k \rangle = \text{const}_{\mathbb{H}}$. Consequently $g = q \in \text{sconst}_G \mathbb{H} \setminus \{0\}$. By Corollary 6.9 it follows that $g = \tilde{g} h$ with $h \in \mathbb{K}[x_1] \dots [x_r]^*$ and $\tilde{g} \in \mathbb{F}^*$ with $\sigma(h) = \lambda u h$ where $\lambda \in \mathbb{K}^*$ is a root of unity. Recall that $\mu' = \text{ford}(u) > 0$ and hence $\mu'' := \text{lcm}(\mu', \text{ord}(\lambda)) > 0$. Since $\sigma^{\mu''}(h) = h$ and (\mathbb{F}, σ) is constant-stable, it follows that $h \in \mathbb{K}^*$. Therefore $g \in \mathbb{K}[x_1] \dots [x_r]^*$. Summarizing, $(m_1, \dots, m_n) \in M(\mathbf{f}, \mathbb{K}[x_1] \dots [x_r])$ and we conclude that $M(\mathbf{f}, \mathbb{E}) \subseteq M(\mathbf{f}, \mathbb{K}[x_1] \dots [x_r])$. The other direction is immediate.

(3) The third part follows by parts 1 and 2 of the corollary and Theorem 3.17. \square

7. The algorithmic machinery III: Problem PFLDE

We aim at proving Theorems 2.23.(2) and 2.26.(3), i.e., providing recursive algorithms that reduce Problem PFLDE from a given $R\Pi\Sigma^*$ -extension to its ground ring (resp. field). If we are considering single-rooted $R\Pi\Sigma^*$ -extensions (Theorem 2.23.(2)), we rely heavily on the fact that for a given difference ring (\mathbb{G}, σ) with constant field \mathbb{K} and given group $G \leq \mathbb{G}^*$ we have that $\text{sconst}_G(\mathbb{G}, \sigma) \setminus \{0\} \leq \mathbb{G}^*$. This property allows us to assume that for any $\mathbf{f} \in \mathbb{G}^n$ and any $u \in G$ the \mathbb{K} -vector space $V = V(u, \mathbf{f}, (\mathbb{G}, \sigma))$ has a basis with dimension $\leq n+1$; see Lemma 2.17. In particular, our reduction algorithm is based on the assumption that there are algorithms available that solve Problems PFLDE and PMT in (\mathbb{G}, σ) for G . For general simple $R\Pi\Sigma^*$ -extensions over a strong constant-stable difference field (\mathbb{G}, σ) (Theorem 2.26.(3)) we need stronger properties: all what we stated above should hold not only for (\mathbb{G}, σ) but must hold for (\mathbb{G}, σ^l) with $l \geq 1$. For the currently explored difference fields (\mathbb{G}, σ) with these properties we refer to Subsection 2.3.3.

7.1. A reduction strategy for $\Pi\Sigma^*$ -extensions

In this subsection we present a reduction method for $\Pi\Sigma^*$ -extensions which can be summarized with the following theorem.

Theorem 7.1. Let (\mathbb{A}, σ) be a computable difference ring and let $G \leq \mathbb{A}^*$ with $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a G -simple $\Pi\Sigma^*$ -extension of (\mathbb{A}, σ) .

- (1) If t is a Σ^* -monomial and Problem PFLDE is solvable in (\mathbb{A}, σ) for G , then Problem PFLDE is solvable in $(\mathbb{A}\langle t \rangle, \sigma)$ for $G_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$.
- (2) If t is a Π -monomial and Problems PFLDE and PMT are solvable in (\mathbb{A}, σ) for G , then Problem PFLDE is solvable in $(\mathbb{A}\langle t \rangle, \sigma)$ for $G_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$.

In the following let $(\mathbb{A}\langle t \rangle, \sigma) \geq (\mathbb{A}, \sigma)$ be a $\Pi\Sigma^*$ -extension as given in the theorem with $\sigma(t) = \alpha t + \beta$ where $\alpha \in G$ and $\beta = 0$, or $\alpha = 1$ and $\beta \in \mathbb{A}$. Furthermore, we define $\tilde{G} = G_{\mathbb{A}}^{\mathbb{A}\langle t \rangle}$ and suppose that we are given a $u \in \tilde{G}$, i.e.,

$$u = v t^m, \quad \text{with } v \in G, m \in \mathbb{Z}, \quad (38)$$

and an $\mathbf{f} = (f_1, \dots, f_n) \in \tilde{G}^n$. By Theorem 3.20 we have that $\text{sconst}_{\tilde{G}} \mathbb{A}\langle t \rangle \setminus \{0\} \leq \mathbb{A}\langle t \rangle^*$ and hence by Lemma 2.17 a basis of $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle)$ with dimension $\leq n+1$ exists. Subsequently, we will prove Theorem 7.1, i.e., we will work out a reduction strategy that provides a basis of $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle)$ under the assumption that one can solve Problem PFLDE in (\mathbb{A}, σ) for G if t is a Σ^* -monomial, resp. Problems PMT and PFLDE in (\mathbb{A}, σ) for G if t is a Π -monomial. The two main steps of this reduction will be described in the following two Subsections 7.1.1 and 7.1.2.

7.1.1. Degree bounds

The first essential step is to search for degree bounds: we will determine $a, b \in \mathbb{Z}$ such that

$$V(u, \mathbf{f}, \mathbb{A}\langle t \rangle_{a,b}) = V(u, \mathbf{f}, \mathbb{A}\langle t \rangle) \quad (39)$$

holds; for the definition of the truncated set of (Laurent) polynomials see (18). For technical reasons we also require that the constraint

$$\max(b, b+m) \geq \tilde{b} \quad (40)$$

holds where m and \tilde{b} are given by (38) and

$$\tilde{b} = \max(\deg(f_1) \dots, \deg(f_n)). \quad (41)$$

The recovery of these bounds (see Lemmas 7.2 and 7.5 below) is based on generalizations of ideas given in [24]; for further details and proofs in the setting of difference fields see also [43, 46].

If t is a Σ^* -monomial, then $\mathbb{A}\langle t \rangle = \mathbb{A}[t]$ forms a polynomial ring, $\alpha = 1$ and $\tilde{G} = G$; in particular we have $m = 0$ in (38). In this case, we can utilize the following lemma.

Lemma 7.2. Let $(\mathbb{A}[t], \sigma)$ be a Σ^* -extension of (\mathbb{A}, σ) and let $G \leq \mathbb{A}^*$ such that $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ holds. Let $f \in \mathbb{A}[t]$ and $u \in G$. Then any solution $g \in \mathbb{A}[t]$ of $\sigma(g) - u g = f$ is bounded by $\deg(g) \leq \max(\deg(f) + 1, 0)$.

Proof. Suppose there is a $g \in \mathbb{A}[t]$ with $\deg(g) > \max(\deg(f) + 1, 0)$. Thus by Lemma 3.8 there is a $\gamma \in \mathbb{A}$ with $\sigma(\gamma) - \gamma = \sigma(t) - t$ which contradicts to Theorem 2.12.(1). \square

Thus we can set $a = 0$ and $b = \max(\tilde{b} + 1, 0)$ to guarantee that (39) and (40) hold.

Example 7.3 (Cont. Ex. 2.15). Consider the Σ^* -extension $(\mathbb{A}[S], \sigma)$ of (\mathbb{A}, σ) with $\mathbb{A} = \mathbb{Q}(k)[x][y][s]$ and $\sigma(S) = S + \frac{xy}{k+1}$ from Example 2.15.(2). As stated in Example 2.15.(3), we want to determine a $g \in \mathbb{A}[S]$ with $\sigma(g) - g = f$ where $f = y k^2 s$, i.e., we want to find a basis of $V(1, \mathbf{f}, \mathbb{A}[S])$ with $\mathbf{f} = (k^2 s y) \in \mathbb{A}[S]^1$. Using Lemma 7.2 it follows that $\deg(g) \leq 1$. Consequently, $V(1, \mathbf{f}, \mathbb{A}[S]) = V(1, \mathbf{f}, \mathbb{A}[S]_0^1)$. Using our methods below (see Example 7.8) we get the basis $\{(1, g), (0, 1)\}$ with g as given in (14).

If t is a Π -monomial, then $\mathbb{A}\langle t \rangle = \mathbb{A}[t, \frac{1}{t}]$ is a ring of Laurent polynomials and $\beta = 0$. First suppose that $u \notin \mathbb{A}$, i.e., $m \in \mathbb{Z} \setminus \{0\}$ as given in (38).

If $f_i = 0$ for all i , it is easy to see that $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle) = V(u, \mathbf{f}, \{0\})$, i.e., $a = 0$ and $b = -1$ fulfil the properties (39) and (40).

Otherwise, if not all f_i are 0, we can use the following fact; the proof is left to the reader.

Lemma 7.4. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a Π -extension of (\mathbb{A}, σ) . Let $v \in \mathbb{A}^*$, $m \in \mathbb{Z} \setminus \{0\}$, $f = \sum_{i=\lambda}^{\mu} f_i t^i \in \mathbb{A}\langle t \rangle$ with $\lambda, \mu \in \mathbb{Z}$ and $g = \sum_{i=\tilde{\lambda}}^{\tilde{\mu}} g_i t^i \in \mathbb{A}\langle t \rangle$ with $\tilde{\lambda}, \tilde{\mu} \in \mathbb{Z}$ and $g_{\tilde{\lambda}} \neq 0 \neq g_{\tilde{\mu}}$ such that $\sigma(g) - v t^m g = f$. Then $\max(\lambda, \lambda - m) \leq \tilde{\lambda}$ and $\tilde{\mu} \leq \min(\mu, \mu - m)$.

Namely, define

$$\tilde{a} = \min(\text{ldeg}(f_1) \dots, \text{ldeg}(f_n)).$$

Note that in this scenario we have that $\tilde{a}, \tilde{b} \in \mathbb{Z}$; for the definition of \tilde{b} see (41). Hence by setting $a = \tilde{a}$ and $b = \tilde{b}$, we can conclude with Lemma 7.4 that (39) and (40) hold.

What remains to consider is the case $u \in G$ with $m = 0$. Here we utilize

Lemma 7.5. Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a Π -extension of (\mathbb{A}, σ) with $G \leq \mathbb{A}^*$ where $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$ and $\alpha = \sigma(t)/t \in G$. Let $u \in G$, $f = \sum_{i=\lambda}^{\mu} f_i t^i \in \mathbb{A}\langle t \rangle$ and $g = \sum_{i=\tilde{\lambda}}^{\tilde{\mu}} g_i t^i \in \mathbb{A}\langle t \rangle$ with $g_{\tilde{\lambda}} \neq 0 \neq g_{\tilde{\mu}}$ and

$$\sigma(g) - u g = f. \quad (42)$$

If there is a $\nu \in \mathbb{Z}$ with

$$\sigma(\gamma) = \alpha^{-\nu} u \gamma \quad (43)$$

for some $\gamma \in \text{sconst}_G \mathbb{A} \setminus \{0\}$, then ν is uniquely determined and we have that $\min(\lambda, \nu) \leq \tilde{\lambda}$ and $\tilde{\mu} \leq \max(\mu, \nu)$. If there is not such a ν , we have that $\lambda \leq \tilde{\lambda}$ and $\tilde{\mu} \leq \mu$.

Proof. Suppose there is a $\nu \in \mathbb{Z}$ with (43) for some $\gamma \in \text{sconst}_G \mathbb{A} \setminus \{0\}$. Take in addition, $\tilde{\nu} \in \mathbb{Z}$ such that $\sigma(\tilde{\gamma}) = \alpha^{-\tilde{\nu}} u \tilde{\gamma}$ holds for some $\tilde{\gamma} \in \text{sconst}_G \mathbb{A} \setminus \{0\}$. Then $\sigma(\gamma/\tilde{\gamma}) = \alpha^{\tilde{\nu}-\nu} \gamma/\tilde{\gamma}$. Since t is a Π -monomial it follows by Theorem 2.12.(2) that $\nu = \tilde{\nu}$, i.e., ν is uniquely determined. Now suppose that there is an i with $g_i \neq 0$ where we have $i < \min(\lambda, \nu)$ or $i > \max(\mu, \nu)$. Then by coefficient comparison in (42) we get $\sigma(g_i) = u \alpha^{-i} g_i$ with $g_i \in \text{sconst}_G \mathbb{A} \setminus \{0\}$. Consequently $\nu = i$, a contradiction. Otherwise, suppose that there is not such a $\nu \in \mathbb{Z}$. Then by the same arguments it follows that $\tilde{\lambda} < \lambda$ or $\tilde{\mu} > \mu$ is not possible, i.e., $\tilde{\lambda} \geq \lambda$ and $\tilde{\mu} \leq \mu$. This completes the proof. \square

Therefore we derive the desired bounds as follows. First, solve Problem PMT and compute a basis of $M((\alpha, u), \mathbb{A})$. Then given a basis, we can decide constructively if there is a $\nu \in \mathbb{Z}$ such that (43) holds. If yes, take the uniquely determined ν and we can take $a = \min(\tilde{a}, \nu)$ and $b = \max(\tilde{b}, \nu)$ to obtain (39) and (40). Otherwise, if there is not such a ν , we can set $a = \min(\tilde{a}, 0)$ and $b = \max(\tilde{b}, -1)$.

Example 7.6 (Cont. Ex. 2.18). Take the difference field $(\mathbb{K}(k)[x]\langle t \rangle, \sigma)$ with $\alpha = \sigma(t)/t = xk$ defined in Example 2.18. In order to find the identity (7), we need a basis of $V = V(u, (0), \mathbb{K}(k)[x]\langle t \rangle)$ with $u = \frac{-x}{k+1} \in G := (\mathbb{K}(k)^*)_{\mathbb{K}(k)}^{\mathbb{K}(k)[x]\langle t \rangle}$; note that $G \leq \mathbb{K}(k)[x]\langle t \rangle^*$ with $\text{sconst}_G \mathbb{K}(k)[x]\langle t \rangle \setminus \{0\} \leq \mathbb{K}(k)[x]\langle t \rangle^*$. In this setting we apply Lemma 7.5. I.e., we compute a basis of $M((\alpha, u), \mathbb{K}(k)[x]) = M((kx, \frac{-x}{k+1}), \mathbb{K}(k)[x])$. As worked out in Example 6.11, a basis is $\{(1, 1)\}$. Thus we find $\nu = -1$ such that there is a $g \in \mathbb{K}(k)[x] \setminus \{0\}$ with (7.5). We conclude that $V = V(u, (0), \mathbb{K}(k)[x]\langle t \rangle_{-1}^{-1})$. Using our methods below (see Example 7.7) we arrive at the basis $(0, x(\iota + x^2)/k/t), (1, 0)$ of V .

Summarizing, we obtain bounds $a, b \in \mathbb{Z}$ such that (39) and (40) hold. For Π -monomials we rely on the extra assumption that Problem PMT is solvable in (\mathbb{A}, σ) for G .

7.1.2. Degree reduction

The following degree reduction has been introduced in [24] in the setting of difference fields. Subsequently, we present the basic ideas in the setting of difference rings; further technical details can be found in [42, Thm. 3.2.2] and [49, 59].

We want to determine all $c_1, \dots, c_n \in \mathbb{K} = \text{const} \mathbb{A}$ and $g_i \in \mathbb{A}$ in $g = \sum_{i=a}^b g_i t_i$ such that the following parameterized equation holds:

$$\sigma(g) - u g = c_1 f_1 + \dots + c_n f_n. \quad (44)$$

If $b < a$, we are in the base case: $g = 0$ and a basis of $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle) = V(u, \mathbf{f}, \{0\})$ can be determined by linear algebra.

Otherwise, we continue as follows. Due to (40), it follows that $\lambda := \max(b, b + m)$ is the highest possible exponent in (44). Let \tilde{f}_i be the coefficient of the term t^λ in f_i . Then by coefficient comparison w.r.t. t^λ in (44) we get the following constraints:

If $m > 0$,

$$-v g_b = c_1 \tilde{f}_1 + \dots + c_n \tilde{f}_n; \quad (45)$$

if $m = 0$,

$$\alpha^b \sigma(g_b) - v g_b = c_1 \tilde{f}_1 + \dots + c_n \tilde{f}_n; \quad (46)$$

if $m < 0$,

$$\alpha^b \sigma(g_b) = c_1 \tilde{f}_1 + \dots + c_n \tilde{f}_n. \quad (47)$$

For the cases $m > 0$ and $m < 0$ one can easily determine a basis of the \mathbb{K} -vector spaces $\{(c_1, \dots, c_n, g_m) \mid (45) \text{ holds}\}$ and $\{(c_1, \dots, c_n, g_m) \mid (47) \text{ holds}\}$ by linear algebra. Moreover, if $m = 0$, equation (46) can be written in the form $\sigma(g_b) - v \alpha^{-b} g_b = c_1 \tilde{f}_1 \alpha^{-b} + \dots + c_n \tilde{f}_n \alpha^{-b}$ where $v \alpha^{-b} \in G$ and $\tilde{f}_i \alpha^{-b} \in \mathbb{A}$. Thus a basis of

$$V(v \alpha^{-b}, (\tilde{f}_1 \alpha^{-b}, \dots, \tilde{f}_n \alpha^{-b}), \mathbb{A}) \quad (48)$$

can be determined under our assumption that one can solve Problem PFLDE in (\mathbb{A}, σ) for G . Now we plug in this partial solution (i.e., the possible leading coefficient g_b with the corresponding linear combinations of the f_i), and end up at a new first-order parameterized difference equation where the highest possible coefficient is $\lambda - 1$. In other words, we reduced the problem by *degree reduction*. We continue to search for the next highest coefficient g_{b-1} . Hence we proceed recursively by updating $\lambda \rightarrow \lambda - 1$ and $b \rightarrow b - 1$ and determine a basis of the reduced problem (with highest degree $\lambda - 1$). Finally, given a basis of this solution space and given the basis of (48), one can determine a basis of $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle_{a,b})$; for further technical details we refer to [24, Thm 12] or [59, Section 3.1]. Summarizing, solving various instances of Problem PFLDE with the degree reductions $b \rightarrow b - 1 \rightarrow \dots \rightarrow a - 1$ leads to the base case and we eventually produce a basis of $V(u, \mathbf{f}, \mathbb{A}\langle t \rangle)$. This concludes the proof of Theorem 7.1.

Example 7.7 (Cont. Ex. 7.6). We know that $g = g_{-1}t^{-1}$. Plugging in g into $\sigma(g) + \frac{x}{k+1} = 0$ yields $\sigma(g_{-1}) + \frac{x^2 k}{k+1} g_{-1} = 0$. Therefore we look for a basis of $V(\frac{-x^2 k}{k+1}, (0), \mathbb{K}(k)[x])$. By using the algorithms presented in Subsection 7.2 we get the basis $\{(1, x(\iota + x^2)/k), (0, 1)\}$. This finally gives the basis $(0, x(\iota + x^2)/k/t), (1, 0)\}$ of $V(\frac{-x}{k+1}, (0), \mathbb{K}(k)[x]\langle t \rangle)$.

Example 7.8 (Cont. Ex. 7.3). We want to find a basis of $V = V(1, \mathbf{f}, \mathbb{A}[S]_0^1)$ with $\mathbb{A} = \mathbb{Q}(k)[x][y][s]$ and $\mathbf{f} = (y k^2 s)$. Hence we make the Ansatz $(c_1, g_0 + g_1 S) \in V$ with the indeterminates $c_1 \in \mathbb{Q}$ and $g_0, g_1 \in \mathbb{A}$ such that

$$\sigma(g_0 + g_1 S) - (g_0 + g_1 S) = c_1 y k^2 s \quad (49)$$

holds. Doing coefficient comparison w.r.t. S^1 yields the constraint $\sigma(g_1) - g_1 = c_1 0$; compare (46). Thus we get all solutions by determining a basis of $V(1, \tilde{\mathbf{f}}, \mathbb{Q}(k)[x][s])$ with $\tilde{\mathbf{f}} = (0) \in \mathbb{A}^1$. In this particular instance, the \mathbb{Q} -basis $\{(1, 0), (0, 1)\}$ is immediate utilizing the fact that the constants are precisely \mathbb{Q} . Summarizing, the solutions are $(c_1, g_1) \in \mathbb{Q}^2$. Consequently, our Ansatz can be refined with $(c_1, g_0 + c_2 S) \in V$ where $c_1 \in \mathbb{Q}$, $c_2 (= g_1) \in \mathbb{Q}$ and $g_0 \in \mathbb{A}$ such that $\sigma(g_0 + c_2 S) - (g_0 + c_2 S) = c_1 k^2 s y$ holds. Bringing the $c_2 S$ part to the right hand side yields the new equation¹⁰

$$\sigma(g_0) - g_0 = c_1 y k^2 s - c_2 h \quad (50)$$

with $h = \sigma(S) - S = \frac{-x y}{k+1} \in \mathbb{A}$. In other words, we need a basis of $V(1, \mathbf{h}, \mathbb{A})$ with $\mathbf{h} = (y k^2 s, \frac{x y}{k+1}) \in \mathbb{A}^2$. Now we apply again the reduction method, but this time in the smaller ring \mathbb{A} without the Σ^* -monomial S . We skip all the details, but refer to a particular subproblem that we will consider in Example 7.13. Finally, we get the basis

$$\{(0, 0, 1), (1, \frac{1}{2}, (\frac{1}{4}(1 - 2k) - \frac{1}{4}x)y + s(\frac{1}{2}(k - 1)(k + 1)x - \frac{1}{2}(k - 2)k)y)\}$$

¹⁰ Note that we reduced the problem to find a polynomial solution of (49) with maximal degree 1 to a polynomial solution of (49) with maximal degree 0. This degree reduction has been achieved by introducing an extra parameter c_2 . In general, the more Σ^* -monomials are involved, the more parameters will be introduced within the proposed degree reduction.

of $V(1, \mathbf{h}, \mathbb{A})$. Thus we can reconstruct the basis $\{(1, g), (0, 1)\}$ of V with g given in (14).

Note that the reduction of Theorem 7.1 simplifies to Karr's field version given in [24] if one specializes \mathbb{A} to a field and sets $G = \mathbb{A}^* = \mathbb{A} \setminus \{0\}$. However, the presented version works not only for a field, but for any difference ring (\mathbb{A}, σ) as specified in Theorem 7.1. Subsequently, we will exploit this enhancement in order to treat (nested) R -extensions.

7.2. A reduction strategy for R -extensions and thus for $R\Pi\Sigma^*$ -extensions

In order to treat simple and single-rooted $R\Pi\Sigma^*$ -extensions (Theorem 2.23.(2)), we utilize the following proposition.

Proposition 7.9. Let (\mathbb{A}, σ) be a computable difference ring with $G \leq \mathbb{A}^*$ and $\text{sconst}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[t], \sigma)$ be an R -extension of (\mathbb{A}, σ) of given order d with $\frac{\sigma(t)}{t} \in G$. Then Problem PFLDE is solvable in $(\mathbb{A}[t], \sigma)$ for G if it is solvable in (\mathbb{A}, σ) for G .

Proof. The proof follows by an adapted degree reduction presented in the proof of Theorem 7.1; see Subsection 7.1.2. Let $u \in G$ and $\mathbf{f} = (f_1, \dots, f_n) \in \mathbb{A}[t]^n$. By definition, it follows that a solution $g \in \mathbb{A}[t]$ and $c_1, \dots, c_n \in \mathbb{K} = \text{const} \mathbb{A}$ of (44) is of the form $g = \sum_{i=a}^b g_i t^i$ with $a := 0$ and $b := d - 1$. Thus the bounds are immediate (under the assumption that d has been determined; see Section 5). Since $\sum_{i=0}^{d-1} h_i t^i = \sum_{i=0}^{d-1} \bar{h}_i t^i$ iff $h_i = \bar{h}_i$, we can activate the degree reduction as outlined in Subsection 7.1.2. Namely, by coefficient comparison of the highest term we always enter in the case (46) (note that $m = 0$ in (38)). By assumption we can solve Problem PFLDE in (\mathbb{A}, σ) for G and thus we can determine a basis of (48). By recursion we finally obtain a basis of $V(u, \mathbf{f}, \mathbb{A}[t])$. \square

Proof 7.10. (Theorem 2.23.(2)). Since Problem PFLDE is solvable in (\mathbb{G}, σ) for G , it follows by iterative applications of Theorem 7.1 and Corollary 4.6.(1) that Problem PFLDE is solvable in (\mathbb{H}, σ) for \tilde{G} with $\mathbb{H} = \mathbb{G}\langle t_1 \rangle \dots \langle t_r \rangle$ and that $\text{sconst}_{\tilde{G}} \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$. Thus by iterative applications of Propositions 7.9 and 3.23 we conclude that Problem PFLDE is solvable in (\mathbb{H}, σ) for \tilde{G} with $\mathbb{H} = \mathbb{H}\langle x_1 \rangle \dots \langle x_u \rangle$ and that $\text{sconst}_{\tilde{G}} \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*$. Finally, by applying iteratively Theorem 7.1 and Corollary 4.6.(1) it follows that Problem PFLDE is solvable in (\mathbb{E}, σ) for \tilde{G} . Note that in Proposition 7.9 we have to know the values $\text{ord}(x_i) = \text{ord}(\alpha_i)$ with $\alpha_i \in G$ (either as input or by computing them first by solving instances of Problem O in G). \square

Finally, we present the underlying reduction method for simple $R\Pi\Sigma^*$ -extensions (Theorem 2.26.(3)) which is based on the following lemma and proposition.

Lemma 7.11. Let (\mathbb{A}, σ) be a difference ring, $f \in \mathbb{A}$, $u \in \mathbb{A}^*$ and $\lambda \in \mathbb{N} \setminus \{0\}$. Then $\sigma(g) - u g = f$ implies that

$$\sigma^\lambda(g) - u_{(\lambda)} g = \sum_{j=0}^{\lambda-1} \frac{u_{(\lambda)}}{u_{(j+1)}} \sigma^j(f). \quad (51)$$

Proof. From $\sigma(g) - u g = f$ we get $\sigma^{j+1}(g) - \sigma^j(u) \sigma^j(g) = \sigma^j(f)$ for all $j \in \mathbb{N}$. Multiplying it with $u_{(\lambda)}/u_{(j+1)}$ yields $\frac{u_{(\lambda)}}{u_{(j+1)}} \sigma^{j+1}(g) - \frac{u_{(\lambda)}}{u_{(j)}} \sigma^j(g) = \frac{u_{(\lambda)}}{u_{(j+1)}} \sigma^j(f)$. Summing this equation over j from 0 to $\lambda - 1$ produces (51). \square

Proposition 7.12. Let (\mathbb{A}, σ) be a constant-stable and computable difference ring with constant field \mathbb{K} . Let $G \leq \mathbb{A}^*$ be closed under σ with $\text{sconst}_G(\mathbb{A}, \sigma^l) \setminus \{0\} \leq \mathbb{A}^*$ for all $l > 0$. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_r \rangle$ be a G -simple R -extension of (\mathbb{A}, σ) where $\text{ord}(x_i) > 0$ and $\text{per}(x_i) > 0$ for $1 \leq i \leq r$ are given and where $\text{sconst}_{(G_{\mathbb{A}}^{\mathbb{E}})} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$. If Problem PFLDE is solvable in (\mathbb{G}, σ^l) for G for all $l > 0$, it is solvable in (\mathbb{E}, σ) for $G_{\mathbb{A}}^{\mathbb{E}}$.

Proof. Let $\mathbb{K} = \text{const} \mathbb{A}$, let $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_r \rangle$, let $\mathbf{f} = (f_1, \dots, f_n) \in \mathbb{E}^n$ and let $u = v x_1^{m_1} \dots x_r^{m_r} \in G_{\mathbb{A}}^{\mathbb{E}}$ with $v \in G$ and $m_i \in \mathbb{N}$. We will present a reduction method to obtain a basis of $V(u, \mathbf{f}, \mathbb{E})$. Set $\alpha := x_1^{m_1} \dots x_r^{m_r}$. Then by Lemma 5.2 it follows that $\text{ord}(\alpha) > 0$ can be computed by the given values of $\text{ord}(x_i)$ with $1 \leq i \leq r$. Hence we can activate Lemma 5.3.(4) and can compute $\text{ford}(\alpha) > 0$. Now take

$$\lambda = \text{lcm}(\text{ford}(\alpha), \text{per}(x_1), \dots, \text{per}(x_r)). \quad (52)$$

Thus we have that ¹¹ $\alpha_{(\lambda)} = 1$ and $\sigma^\lambda(x_i) = x_i$ for all $1 \leq i \leq r$. Finally, define

$$w := u_{(\lambda)} = (\alpha v)_{(\lambda)} = v_{(\lambda)} \in G. \quad (53)$$

Now let $(c_1, \dots, c_n, g) \in V(u, \mathbf{f}, \mathbb{E})$, i.e., we have that (44). Thus Lemma 7.11 yields

$$\sigma^\lambda(g) - w g = c_1 \tilde{f}_1 + \dots + c_n \tilde{f}_n \quad (54)$$

with

$$\tilde{f}_i = \sum_{j=0}^{\lambda-1} \frac{u_{(\lambda)}}{u_{(j+1)}} \sigma^j(f_i). \quad (55)$$

Hence $V(u, \mathbf{f}, \mathbb{E})$ is a subset of

$$\tilde{V} = \{(c_1, \dots, c_n, g) \in \mathbb{K}^n \times \mathbb{E} \mid (54) \text{ holds}\}. \quad (56)$$

Note that \tilde{V} is a \mathbb{K} -subspace of $\mathbb{K}^n \times \mathbb{E}$. Thus $V(u, \mathbf{f}, \mathbb{E})$ is a subspace of \tilde{V} over \mathbb{K} . First, we show that \tilde{V} has a finite basis and show how one can compute it. For this task define $S := \{(n_1, \dots, n_r) \in \mathbb{N}^r \mid 0 \leq n_i < \text{ord}(x_i)\}$. Write $g = \sum_{\mathbf{i} \in S} g_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ and $\tilde{f}_j = \sum_{\mathbf{i} \in S} \tilde{f}_{j,\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ in multi-index notation. Since $\sigma^\lambda(x_i) = x_i$, it follows by coefficient comparison that for $\mathbf{i} \in S$ we have that

$$\sigma^\lambda(g_{\mathbf{i}}) - w g_{\mathbf{i}} = c_1 \tilde{f}_{1,\mathbf{i}} + \dots + c_n \tilde{f}_{n,\mathbf{i}}.$$

By assumption, $\text{sconst}_G(\mathbb{A}, \sigma^\lambda) \setminus \{0\} \leq \mathbb{A}^*$. In particular, since (\mathbb{A}, σ) is constant-stable, we have that $\text{const}(\mathbb{A}, \sigma^\lambda) = \mathbb{K}$. Thus with our $w \in G$ and $\tilde{\mathbf{f}}_{\mathbf{i}} = (\tilde{f}_{1,\mathbf{i}}, \dots, \tilde{f}_{n,\mathbf{i}}) \in \mathbb{A}^n$ we can solve Problem PFLDE in $(\mathbb{A}, \sigma^\lambda)$ with constant field \mathbb{K} . Hence we get for all $\mathbf{i} \in S$ the bases for

$$V_{\mathbf{i}} = V(w, \tilde{\mathbf{f}}_{\mathbf{i}}, (\mathbb{A}, \sigma^\lambda)). \quad (57)$$

Note that by construction it follows that \tilde{V} from (56) is given by

$$\tilde{V} = \{(c_1, \dots, c_n, \sum_{\mathbf{i} \in S} g_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}) \mid (c_1, \dots, c_n, g_{\mathbf{i}}) \in V_{\mathbf{i}}\}. \quad (58)$$

Thus by linear algebra we get a basis of (58), say $\mathbf{b}_1, \dots, \mathbf{b}_s \in \mathbb{K}^n \times \mathbb{E}$. Recall that $V(u, \mathbf{f}, (\mathbb{E}, \sigma))$ is a \mathbb{K} -subspace of (58). To this end, we make the Ansatz $(c_1, \dots, c_n, g) = d_1 \mathbf{b}_1 + \dots + d_s \mathbf{b}_s$ for indeterminates $d_1, \dots, d_s \in \mathbb{K}$ and plug in the generic solution into (44). This yields another linear system with unknowns (d_1, \dots, d_s) . Solving this system enables one to derive a basis of $V(u, \mathbf{f}, \mathbb{E})$. \square

¹¹ By a mild modification of the proof it suffices to take a λ such that $\alpha_{(\lambda)} \in \text{const} \mathbb{A}$ holds.

Example 7.13 (Cont. Ex. 7.8). In order to compute a basis of $V(1, \mathbf{h}, \mathbb{A})$ in Ex. 7.8, the recursive reduction enters in the following subproblem. We are given the R -extension $(\mathbb{Q}(k)[x], \sigma)$ of $(\mathbb{Q}(k), \sigma)$ with $\sigma(x) = -x$ and need a basis of $V(x, \mathbf{f}, \mathbb{Q}(k)[x])$ with $\mathbf{f} = (f_1, f_2, f_3) = (\frac{(k^2-1)x}{2k} + \frac{-k^2-2k}{2k}, -\frac{x}{k}, 0)$. By Example 5.4.(2) we get $\text{per}(x) = 2$ and $\text{ford}(x) = 4$. Hence using (52) we determine $\lambda = \text{lcm}(\text{ford}(x), \text{per}(x)) = 4$. Using (55) with $u = x$ yields $(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3) = (-\frac{2k^2+4k+1}{k(k+2)} - \frac{x}{(k+1)(k+3)}, -\frac{2x}{(k+1)(k+3)} - \frac{2}{k(k+2)}, 0)$. Next we write the entries in multi-index notation. Namely, with $S = \{(0), (1)\} \subseteq \mathbb{N}^1$ we get

$$\begin{aligned}\tilde{\mathbf{f}}_{(0)} &= (\tilde{f}_{1,(0)}, \tilde{f}_{2,(0)}, \tilde{f}_{3,(0)}) = (-\frac{2k^2+4k+1}{k(k+2)}, -\frac{2}{k(k+2)}, 0) \\ \tilde{\mathbf{f}}_{(1)} &= (\tilde{f}_{1,(1)}, \tilde{f}_{2,(1)}, \tilde{f}_{3,(1)}) = (-\frac{1}{(k+1)(k+3)}, -\frac{2}{(k+1)(k+3)}, 0)\end{aligned}$$

with $\mathbf{f} = \sum_{(m) \in S} \tilde{\mathbf{f}}_{(m)} x^m = \tilde{\mathbf{f}}_{(0)} + \tilde{\mathbf{f}}_{(1)} x$. Following (53) we get $w = 1$ and we have to compute bases of the (57) with $\mathbf{i} \in S$. Here we obtain the basis $\{(0, 0, 1, 0), (1, -\frac{1}{2}, 0, -k/2)\}$ of $V_{(0)} = V(1, \tilde{\mathbf{f}}_{(0)}, (\mathbb{Q}(k), \sigma^4))$ and the basis $\{(-1, \frac{1}{2}, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0)\}$ of $V_{(1)} = V(1, \tilde{\mathbf{f}}_{(1)}, (\mathbb{Q}(k), \sigma^4))$. Therefore a basis of

$$\begin{aligned}\tilde{V} &= \{(c_1, c_2, c_3, g) \in \mathbb{Q}^3 \times \mathbb{Q}(k)[x] \mid \sigma^4(g) - g = c_1 \tilde{f}_1 + c_2 \tilde{f}_2 + c_3 \tilde{f}_3\} \\ &= \{(c_1, c_2, c_3, \sum_{(i) \in \{(0), (1)\}} g_i x^i) \mid (c_1, c_2, c_3, g_{(i)}) \in V_{(i)}\}\end{aligned}$$

can be read off: $\{(1, -1/2, 0, -k/2), (0, 0, 1, 0), (0, 0, 0, 1)\}$. Since $V(x, \mathbf{f}, \mathbb{Q}(k)[x])$ is a \mathbb{Q} -subspace of \tilde{V} , we plug in $(c_1, c_2, c_3, g) = d_1(1, -1/2, 0, -\frac{k}{2}) + d_2(0, 0, 1, 0) + d_3(0, 0, 0, 1) + d_4(0, 0, 0, 1)$ with unknowns $d_1, d_2, d_3, d_4 \in \mathbb{Q}$ into (44). Together with our given f_i and u we get the linear constraint $\frac{1}{2}(d_1 - 2d_3 + 2d_4) + x(-d_3 - d_4) = 0$ or equivalently the linear constraints $-d_3 - d_4 = 0$ and $\frac{1}{2}(d_1 - 2d_3 + 2d_4)$. This yields $d_3 = \frac{d_1}{4}$ and $d_4 = -\frac{d_1}{4}$. Thus we obtain the generic solution $d_1(1, -\frac{1}{2}, 0, -\frac{k}{2} + \frac{x}{4} - \frac{1}{4}) + d_2(0, 0, 1, 0)$ of $V(x, \mathbf{f}, \mathbb{Q}(k)[x])$, i.e., the basis $\{(1, -\frac{1}{2}, 0, -\frac{k}{2} + \frac{x}{4} - \frac{1}{4}), (0, 0, 1, 0)\}$ of $V(x, \mathbf{f}, \mathbb{Q}(k)[x])$.

Remark 7.14. (1) In the underlying algorithm of Proposition 7.12 we construct for all $\mathbf{i} \in S$ the solution spaces given in (57) and combine them in one stroke as proposed in (58). This approach is interesting if one wants to perform calculations in parallel. Another approach is to apply similar tactics as given in Subsection 7.1: compute a basis of one of the (57), plug in the found solutions and continue with an updated Ansatz in terms of the remaining monomials. In this way, one usually shortens step by step the length of the vectors $\tilde{\mathbf{f}}_{\mathbf{i}}$ in (57) and ends up very soon at a trivial situation (shortcut).

(2) A different approach is to consider an R -extension $(\mathbb{F}[x], \sigma)$ of (\mathbb{F}, σ) of order d as a holonomic expression [61,15,30] over a difference field. Then as worked out in [47,17], a solution $g = \sum_{i=0}^{d-1} g_i x^i$ and $c_i \in \text{const } \mathbb{F}$ of (9) leads to a coupled system of first-order difference equations in terms of the g_i that can be uncoupled explicitly. More precisely, there is an explicitly given formula that constitutes a higher-order parameterized linear difference equation in g_{d-1} and the parameters c_i . Solving this difference equation in terms of g_{d-1} and the c_i delivers automatically the remaining coefficients g_i , i.e., the solution g of (9). Here one usually has to solve a general higher-order linear difference equation. For further details on the holonomic Ansatz in the context of algebraic ring extensions (also on handling such objects in the basis of idempotent elements [60,19]) we refer to [17].

The advantage of the reduction technique proposed in Proposition 7.12 is that it can be applied in one stroke for nested R -extensions. In particular, Problem PFLDE can be always reduced again to Problem PFLDE by possibly switching to (\mathbb{F}, σ^k) for some $k > 1$. In this way, general higher-order linear difference equations can be avoided.

Combining all algorithmic parts of this article we obtain the following result.

Theorem 7.15. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}\langle t_1 \rangle \dots \langle t_e \rangle$ be a simple $R\Pi\Sigma^*$ -extension of a constant-stable and computable field (\mathbb{F}, σ) . Suppose that for all R -monomials the periods are positive, and the orders and periods of the R -monomials are given explicitly. Then Problem PFLDE in (\mathbb{E}, σ) for $(\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$ is solvable if one of the following holds.

- (1) All t_i are $R\Sigma^*$ -monomials and PFLDE is solvable in (\mathbb{F}, σ^k) for \mathbb{F}^* for all $k > 0$.
- (2) Problem PMT is solvable in (\mathbb{F}, σ) for \mathbb{F}^* and Problem PFLDE is solvable in (\mathbb{F}, σ^k) for \mathbb{F}^* for all $k > 0$.

Proof. Let $H = (\mathbb{F}^*)_{\mathbb{F}}^{\mathbb{E}}$. Recall that by Theorem 2.24 we have that $\text{sconst}_H \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$, i.e., Problem PFLDE is applicable in (\mathbb{E}, σ) for H . By Lemma 4.10 we can reorder the generators of the $R\Pi\Sigma^*$ -extension such that $(\bar{\mathbb{E}}, \sigma)$ is an \mathbb{F}^* -simple R -extension of (\mathbb{F}, σ) and $(\bar{\mathbb{E}}, \sigma)$ is a G -simple $\Pi\Sigma^*$ -extension of $(\bar{\mathbb{E}}, \sigma)$ with $G = (\mathbb{F}^*)_{\mathbb{F}}^{\bar{\mathbb{E}}}$. Note that the multiplicative group \mathbb{F}^* is closed under σ , $\text{sconst}_{(\mathbb{F}^*)}(\mathbb{F}, \sigma^l) = \mathbb{F}^*$ for all $l > 0$ and $\text{sconst}_{(\mathbb{F}^*)} \bar{\mathbb{E}} \setminus \{0\} \leq \mathbb{E}^*$ by Corollary 4.3. Thus we can apply Proposition 7.12. Hence Problem PFLDE is solvable in $(\bar{\mathbb{E}}, \sigma)$ for G . If we are in case (1), i.e., no Π -monomials occur, we can apply iteratively Theorem 7.1 and obtain an algorithm to solve Problem PFLDE in (\mathbb{E}, σ) for $G_{\bar{\mathbb{E}}}^{\mathbb{E}} = H$. If we are in case (2), i.e., Π -monomials may occur, we exploit in addition our assumptions together with Theorem 2.26.(2). This shows that we can solve Problem PMT in (\mathbb{E}, σ) for H (and in any sub-difference ring by truncating the tower of extensions). Again the iterative application of Theorem 7.1 shows that Problem PFLDE is solvable in (\mathbb{E}, σ) for $G_{\bar{\mathbb{E}}}^{\mathbb{E}} = H$. \square

Proof 7.16. (Theorem 2.26.(3)). Let (\mathbb{E}, σ) be a simple $R\Pi\Sigma^*$ -extension of (\mathbb{F}, σ) where (\mathbb{F}, σ) is computable and strong constant-stable. Then by Corollary 5.6 (parts 3 and 4) the periods and orders of all R -monomials are positive and can be computed. Thus Theorem 7.15.(2) is applicable which completes the proof. \square

We remark that in Theorem 2.26.(3) one can drop the condition that Problem PMT is solvable in (\mathbb{F}, σ) for \mathbb{F}^* if in the $R\Pi\Sigma^*$ -extension no Π -monomials occur, i.e., one applies part one and not part two of Theorem 7.15.

8. Conclusion

We provided important building blocks that extend the well established difference field theory to a difference ring theory. In this setting one can handle in addition objects such as (4). We elaborated algorithms for the (multiplicative) telescoping problem (Problems T and MT) and the (multiplicative) parameterized telescoping problem (Problems PT and PMT). In particular, Problem PT enables one to apply Zeilberger's creative telescoping paradigm in the rather general class of simple $R\Pi\Sigma^*$ -extensions. In order to derive these algorithms we showed that certain semi-constants (resp. semi-invariants) of the difference rings under consideration form a multiplicative group.

Currently, the underlying engine of Theorem 2.23 with the ground field machinery of Subsection 2.3.3 is fully implemented within the summation package¹² **Sigma**. In this way one can treat big classes of indefinite nested sums and products involving algebraic objects like $(-1)^k$. In particular, one can treat d'Alembertian solutions of linear recurrences as worked out in Subsection 2.4. We emphasize that these algorithms are enhanced by the refinements described in [45,48,51,53,8,59] in order to find sum representations with certain optimality criteria, like optimal nesting depth.

The machinery to handle nested R -extensions (see Theorem 2.26) is not incorporated in **Sigma** yet. First, further investigations will be necessary so that the new algorithms can be merged with the difference field enhancements of **Sigma**.

Another challenging task is to push forward the difference ring theory and the underlying algorithms in order to relax the requirements in Theorems 2.23 and 2.26 that the $R\Pi\Sigma^*$ -extensions are simple and/or that the ground difference ring is strong constant-stable. In this regard, we refer to the comments given in Example 2.20.

In any case, the currently developed toolbox widens the class of indefinite nested sums and products in the setting of difference rings. We are looking forward to see new kinds of applications that can be attacked with this machinery.

Acknowledgement

I would like to thank Michael Singer and the anonymous referee for their helpful comments and suggestions to improve the presentation of this article.

Appendix: A short index

$M(\mathbf{f}, \mathbb{A})$, 10	ring/field, 4
$V(u, \mathbf{f}, \mathbb{A})$, 11	ring/field extension, 5
$\mathbb{A}\langle t \rangle$, 7	
$\mathbb{A}\langle t \rangle_{a,b}$, 17	extension
\deg , 17	(nested) $\Pi, \Sigma^*, R, R\Pi$,
$(\mathbb{A}, \sigma) \leq (\tilde{A}, \tilde{\sigma})$, 5	$R\Sigma^*, \Pi\Sigma^*, R\Pi\Sigma^*$, 7
$G_{\mathbb{G}}^{\mathbb{A}}$, 12	Π , 5
$\text{ford}(f)$, 27	R , 7
$\text{sconst}(\mathbb{A}, \sigma)$, $\text{sconst}\mathbb{A}$, 10	Σ^* , 5
$\langle S \rangle$, 4	algebraic, 6
ldeg , 17	simple, G -simple, 12
$\text{ord}(f)$, 6	single-rooted, 13
$\text{per}(f)$, 27	unimonomial, 5
$\text{sconst}_G(\mathbb{A}, \sigma)$, $\text{sconst}_G\mathbb{A}$, 10	
$f_{(k,\sigma)}, f_{(k)}$, 17	function
$\Pi\Sigma^*$ -field, 7	degree, 17
	factorial order, 27
constant field/ring, 4	order, 6
	period, 27
difference	rising factorial, 17

¹²The **Sigma** package can be downloaded from www.risc.jku.at/research/combinat/software/Sigma/

monomial	T, 4
$\Pi, \Sigma^*, R, R\Pi, R\Sigma^*, \Pi\Sigma^*, R\Pi\Sigma^*$, 7	product group, 12
simple, G -simple, 12	
Problem	ring
FPLDE, 11	(strong) constant-stable, 14
MT, 8	connected, 16
O, 8	constant-stable, 14
PMT, 11	reduced, 16
PT, 4	semi-constant, 10

References

- [1] J. Ablinger, A. Behring, J. Blümlein, A. De Freitas, A. Hasselhuhn, A. von Manteuffel, M. Round, C. Schneider, and F. Wissbrock. The 3-loop non-singlet heavy flavor contributions and anomalous dimensions for the structure function $F_2(x, Q^2)$ and transversity. *Nucl. Phys. B*, 886:733–823, 2014. arXiv:1406.4654 [hep-ph].
- [2] J. Ablinger, J. Blümlein, A. De Freitas, A. Hasselhuhn, A. von Manteuffel, M. Round, C. Schneider, and F. Wissbrock. The transition matrix element $A_{gq}(N)$ of the variable flavor number scheme at $O(\alpha_s^3)$. *Nucl. Phys. B*, 882:263–288, 2014. arXiv:1402.0359 [hep-ph].
- [3] J. Ablinger, J. Blümlein, and C. Schneider. Harmonic sums and polylogarithms generated by cyclotomic polynomials. *J. Math. Phys.*, 52(10):1–52, 2011. [arXiv:1007.0375 [hep-ph]].
- [4] J. Ablinger, J. Blümlein, and C. Schneider. Analytic and algorithmic aspects of generalized harmonic sums and polylogarithms. *J. Math. Phys.*, 54(8):1–74, 2013. arXiv:1302.0378 [math-ph].
- [5] S. A. Abramov. On the summation of rational functions. *Zh. vychisl. mat. Fiz.*, 11:1071–1074, 1971.
- [6] S. A. Abramov, M. Bronstein, M. Petkovšek, and C. Schneider. *In preparation*, 2015.
- [7] S. A. Abramov and M. Petkovšek. D’Alembertian solutions of linear differential and difference equations. In J. von zur Gathen, editor, *Proc. ISSAC’94*, pages 169–174. ACM Press, 1994.
- [8] S. A. Abramov and M. Petkovšek. Polynomial ring automorphisms, rational (w, σ) -canonical forms, and the assignment problem. *J. Symbolic Comput.*, 45(6):684–708, 2010.
- [9] A. Bauer and M. Petkovšek. Multibasic and mixed hypergeometric Gosper-type algorithms. *J. Symbolic Comput.*, 28(4–5):711–736, 1999.
- [10] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.
- [11] J. Blümlein, A. Hasselhuhn, S. Klein, and C. Schneider. The $O(\alpha_s^3 n_f T_F^2 C_{A,F})$ contributions to the gluonic massive operator matrix elements. *Nucl. Phys. B*, 866:196–211, 2013. [arXiv:1205.4184 [hep-ph]].
- [12] J. Blümlein, S. Klein, C. Schneider, and F. Stan. A symbolic summation approach to Feynman integral calculus. *J. Symbolic Comput.*, 47:1267–1289, 2012.
- [13] M. Bronstein. *Symbolic Integration I, Transcendental functions*. Springer, Berlin-Heidelberg, 1997.
- [14] M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. *J. Symbolic Comput.*, 29(6):841–877, 2000.
- [15] F. Chyzak. An extension of Zeilberger’s fast algorithm to general holonomic functions. *Discrete Math.*, 217:115–134, 2000.
- [16] R. M. Cohn. *Difference Algebra*. Interscience Publishers, John Wiley & Sons, 1965.

- [17] B. Eröcal. *Algebraic extensions for summation in finite terms*. PhD thesis, RISC, Johannes Kepler University, Linz, February 2011.
- [18] R. W. Gosper. Decision procedures for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75:40–42, 1978.
- [19] C. Hardouin and M.F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [20] P. A. Hendriks and M. F. Singer. Solving difference equations in finite terms. *J. Symbolic Comput.*, 27(3):239–259, 1999.
- [21] M. van Hoeij. Finite singularities and hypergeometric solutions of linear recurrence equations. *J. Pure Appl. Algebra*, 139(1-3):109–131, 1999.
- [22] P. Horn, W. Koepf, and T. Sprenger. m -fold hypergeometric solutions of linear recurrence equations revisited. *Math. Comput. Sci.*, 6(1):61–77, 2012.
- [23] G. Karpilovsky. On finite generation of unit groups of commutative group rings. *Arch. Math. (Basel)*, 40(6):503–508, 1983.
- [24] M. Karr. Summation in finite terms. *J. ACM*, 28:305–350, 1981.
- [25] M. Karr. Theory of summation in finite terms. *J. Symbolic Comput.*, 1:303–315, 1985.
- [26] M. Kauers and P. Paule. *The concrete tetrahedron*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, 2011. Symbolic sums, recurrence equations, generating functions, asymptotic estimates.
- [27] M. Kauers and C. Schneider. Application of unspecified sequences in symbolic summation. In J.G. Dumas, editor, *Proc. ISSAC’06*, pages 177–183. ACM Press, 2006.
- [28] M. Kauers and C. Schneider. Indefinite summation with unspecified summands. *Discrete Math.*, 306(17):2021–2140, 2006.
- [29] M. Kauers and C. Schneider. Symbolic summation with radical expressions. In C.W. Brown, editor, *Proc. ISSAC’07*, pages 219–226, 2007.
- [30] C. Koutschan. Creative telescoping for holonomic functions. In C. Schneider and J. Blümlein, editors, *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, pages 171–194. Springer, 2013. arXiv:1307.4554 [cs.SC].
- [31] A. Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
- [32] Erhard Neher. Invertible and nilpotent elements in the group algebra of a unique product group. *Acta Appl. Math.*, 108(1):135–139, 2009.
- [33] R. Osburn and C. Schneider. Gaussian hypergeometric series and extensions of supercongruences. *Math. Comp.*, 78(265):275–292, 2009.
- [34] P. Paule. Greatest factorial factorization and symbolic summation. *J. Symbolic Comput.*, 20(3):235–268, 1995.
- [35] P. Paule and A. Riese. A Mathematica q -analogue of Zeilberger’s algorithm based on an algebraically motivated approach to q -hypergeometric telescoping. In M. Ismail and M. Rahman, editors, *Special Functions, q -Series and Related Topics*, volume 14, pages 179–210. AMS, 1997.
- [36] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symbolic Comput.*, 14(2-3):243–264, 1992.
- [37] M. Petkovšek, H. S. Wilf, and D. Zeilberger. *$A = B$* . A. K. Peters, Wellesley, MA, 1996.
- [38] M. Petkovšek and H. Zakrajšek. Solving linear recurrence equations with polynomial coefficients. In C. Schneider and J. Blümlein, editors, *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, pages 259–284. Springer, 2013.
- [39] H. Prodinger, C. Schneider, and S. Wagner. Unfair permutations. *Europ. J. Comb.*, 32:1282–1298, 2011.

- [40] R. Risch. The problem of integration in finite terms. *Trans. Amer. Math. Soc.*, 139:167–189, 1969.
- [41] C. Schneider. An Implementation of Karr’s Summation Algorithm in Mathematica. *Sém. Lothar. Combin.*, S43b:1–10, 2000.
- [42] C. Schneider. Symbolic summation in difference fields. Technical Report 01-17, RISC-Linz, J. Kepler University, November 2001. PhD Thesis.
- [43] C. Schneider. A collection of denominator bounds to solve parameterized linear difference equations in $\Pi\Sigma$ -extensions. *An. Univ. Timișoara Ser. Mat.-Inform.*, 42(2):163–179, 2004. Extended version of Proc. SYNASC’04.
- [44] C. Schneider. The summation package Sigma: Underlying principles and a rhombus tiling application. *Discrete Math. Theor. Comput. Sci.*, 6:365–386, 2004.
- [45] C. Schneider. Symbolic summation with single-nested sum extensions. In J. Gutierrez, editor, *Proc. ISSAC’04*, pages 282–289. ACM Press, 2004.
- [46] C. Schneider. Degree bounds to find polynomial solutions of parameterized linear difference equations in $\Pi\Sigma$ -fields. *Appl. Algebra Engrg. Comm. Comput.*, 16(1):1–32, 2005.
- [47] C. Schneider. A new Sigma approach to multi-summation. *Adv. in Appl. Math.*, 34(4):740–767, 2005.
- [48] C. Schneider. Product representations in $\Pi\Sigma$ -fields. *Ann. Comb.*, 9(1):75–99, 2005.
- [49] C. Schneider. Solving parameterized linear difference equations in terms of indefinite nested sums and products. *J. Differ. Equations Appl.*, 11(9):799–821, 2005.
- [50] C. Schneider. Apéry’s double sum is plain sailing indeed. *Electron. J. Combin.*, 14, 2007.
- [51] C. Schneider. Simplifying sums in $\Pi\Sigma$ -extensions. *J. Algebra Appl.*, 6(3):415–441, 2007.
- [52] C. Schneider. Symbolic summation assists combinatorics. *Sém. Lothar. Combin.*, 56:1–36, 2007. Article B56b.
- [53] C. Schneider. A refined difference field theory for symbolic summation. *J. Symbolic Comput.*, 43(9):611–644, 2008. [arXiv:0808.2543v1].
- [54] C. Schneider. Parameterized telescoping proves algebraic independence of sums. *Ann. Comb.*, 14(4):533–552, 2010. [arXiv:0808.2596].
- [55] C. Schneider. Structural theorems for symbolic summation. *Appl. Algebra Engrg. Comm. Comput.*, 21(1):1–32, 2010.
- [56] C. Schneider. A symbolic summation approach to find optimal nested sum representations. In A. Carey, D. Ellwood, S. Paycha, and S. Rosenberg, editors, *Motives, Quantum Field Theory, and Pseudodifferential Operators*, volume 12 of *Clay Mathematics Proceedings*, pages 285–308. Amer. Math. Soc, 2010. arXiv:0808.2543.
- [57] C. Schneider. Simplifying multiple sums in difference fields. In C. Schneider and J. Blümlein, editors, *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, pages 325–360. Springer, 2013. arXiv:1304.4134 [cs.SC].
- [58] C. Schneider. Modern summation methods for loop integrals in quantum field theory: The packages Sigma, EvaluateMultiSums and SumProduction. In *Proc. ACAT 2013*, volume 523 of *J. Phys.: Conf. Ser.*, pages 1–17, 2014. arXiv:1310.0160 [cs.SC].
- [59] C. Schneider. Fast algorithms for refined parameterized telescoping in difference fields. In M. Weimann J. Guitierrez, J. Schicho, editor, *Computer Algebra and Polynomials, Applications of Algebra and Number Theory*, Lecture Notes in Computer Science (LNCS), pages 157–191. Springer, 2015. arXiv:1307.7887 [cs.SC].
- [60] M. van der Put and M.F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
- [61] D. Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32:321–368, 1990.
- [62] D. Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11:195–204, 1991.